QLOGIC

Simplify

SANbox 5000 Series Fibre Channel Switch

Command Line Interface Guide

Firmware Version 6.7

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

This SANbox switch is covered by one or more of the following patents: 6697359; other patents pending.

QLogic and SANbox are trademarks or registered trademarks of QLogic Corporation.

Microsoft, Windows NT, and Windows 2000/2003, and Internet Explorer are registered trademarks of Microsoft Corporation.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History	
Release, Revision A, July 25, 2007	Firmware Version 6.7 Enterprise Fabric Suite 2007 version 6.07

© 2000–2007 QLogic Corporation. All Rights Reserved Worldwide.
First Published: December 2005

QLogic Corporation, 26650 Aliso Viejo Parkway, Aliso Viejo, CA 92656, (800) 662-4471 or (949) 389-6000

Table of Contents

Section 1 Introduction

1.1 Switch Models and Examples 1-2
1.2 Intended Audience 1-2
1.3 Related Materials 1-2
1.4 New in This Release 1-3
1.5 Technical Support 1-4
1.5.1 Availability 1-4
1.5.2 Training 1-4
1.5.3 Contact Information 1-5

Section 2 Command Line Interface Usage

2.1 Logging In to the Switch 2-2
2.2 Opening and Closing an Admin Session 2-3
2.3 Entering Commands 2-3
2.4 Getting Help 2-4
2.5 Setting Page Breaks 2-4
2.6 Creating a Support File 2-5
2.7 Downloading and Uploading Files 2-7

Section 3 User Account Configuration

3.1 Displaying User Account Information 3-2
3.2 Creating User Accounts 3-3
3.3 Modifying User Accounts and Passwords 3-4

Section 4 Network and Fabric Configuration

4.1 Displaying Name Server Information 4-2
4.2 Displaying the Ethernet Network Configuration 4-3
4.3 Configuring the Ethernet Port 4-4
4.4 Verifying a Switch in the Network 4-5
4.5 Verifying and Tracing Fibre Channel Connections 4-5

Section 5 Switch Configuration

5.1 Displaying Switch Information 5-1
5.1.1 Switch Operational Information 5-2
5.1.2 System Process Information 5-3
5.1.3 Elapsed Time Between Resets 5-4

5.1.4 Configuration Information 5-5
5.1.4.1 Switch Configuration Parameters 5-5
5.1.4.2 Zoning Configuration Parameters 5-6
5.1.4.3 Security Configuration Parameters 5-6
5.1.5 Hardware Information 5-7
5.1.6 Firmware Information 5-8
5.2 Managing Switch Services 5-9
5.3 Managing Switch Configurations 5-11
5.3.1 Display a List of Switch Configurations 5-11
5.3.2 Activate a Switch Configuration 5-11
5.3.3 Copy a Switch Configuration 5-12
5.3.4 Delete a Switch Configuration 5-12
5.3.5 Modify a Switch Configuration 5-12
5.3.6 Back Up and Restore a Switch Configuration 5-14
5.3.6.1 Creating the Backup File 5-14
5.3.6.2 Downloading the Configuration File 5-15
5.3.6.3 Restoring the Configuration File 5-16
5.4 Paging a Switch 5-17
5.5 Setting the Date and Time 5-17
5.6 Resetting a Switch 5-20
5.7 Installing Firmware 5-20
5.7.1 Nondisruptive Activation 5-21
5.7.2 One-Step Firmware Installation 5-21
5.7.3 Custom Firmware Installation 5-23
5.8 Managing Switch Feature Upgrades 5-24
5.8.1 Display Feature Licenses 5-24
5.8.2 Install a Feature License Key 5-25

Section 6 Port Configuration

6.1 Displaying Port Information 6-1
6.1.1 Port Configuration Parameters 6-2
6.1.2 Port Operational Information 6-3
6.1.3 Port Threshold Alarm Configuration Parameters 6-4
6.1.4 Port Performance 6-5
6.1.5 Transceiver Information 6-6
6.2 Modifying Port Operating Characteristics 6-7
6.3 Port Binding 6-8
6.4 Resetting a Port 6-9
6.5 Configuring Port Threshold Alarms 6-10
6.6 Testing a Port 6-12

6.6.1 Online Tests for Ports 6-12
6.6.2 Offline Tests for Ports 6-13
6.6.3 Display Port Test Results 6-14
6.6.4 Cancel a Port Test 6-14
6.7 Extending Port Transmission Distance 6-15

Section 7 Zoning Configuration

7.1 Displaying Zoning Database Information 7-2
7.1.1 Configured Zone Set Information 7-2
7.1.2 Active Zone Set Information 7-4
7.1.3 Zone Set Membership Information 7-5
7.1.4 Zone Membership Information 7-5
7.1.5 Alias and Alias Membership Information 7-6
7.1.6 Zoning Modification History 7-7
7.1.7 Zoning Database Limits 7-8
7.2 Configuring the Zoning Database 7-9
7.3 Modifying the Zoning Database 7-11
7.4 Resetting the Zoning Database 7-12
7.5 Removing Inactive Zone Sets, Zones, and Aliases 7-12
7.6 Managing Zone Sets 7-13
7.6.1 Create a Zone Set 7-13
7.6.2 Delete a Zone Set 7-13
7.6.3 Rename a Zone Set 7-14
7.6.4 Copy a Zone Set 7-14
7.6.5 Add Zones to a Zone Set 7-14
7.6.6 Remove Zones from a Zone Set 7-14
7.6.7 Activate a Zone Set 7-14
7.6.8 Deactivate a Zone Set 7-15
7.7 Managing Zones 7-15
7.7.1 Create a Zone 7-15
7.7.2 Delete a Zone 7-15
7.7.3 Rename a Zone 7-16
7.7.4 Copy a Zone 7-16
7.7.5 Add Members to a Zone 7-16
7.7.6 Remove Members from a Zone 7-16
7.8 Managing Aliases 7-17
7.8.1 Create an Alias 7-17
7.8.2 Delete an Alias 7-17
7.8.3 Rename an Alias 7-17
7.8.4 Copy an Alias 7-18

7.8.5 Add Members to an Alias 7-18
7.8.6 Remove Members from an Alias 7-18

Section 8 Connection Security Configuration

8.1 Managing SSL and SSH Services 8-1
8.2 Displaying SSL and SSH Services 8-3
8.3 Creating an SSL Security Certificate 8-3

Section 9 Device Security Configuration

9.1 Displaying Security Database Information 9-2
9.1.1 Configured Security Set Information 9-2
9.1.2 Active Security Set Information 9-4
9.1.3 Security Set Membership Information 9-5
9.1.4 Group Membership Information 9-5
9.1.5 Security Database Modification History 9-6
9.1.6 Security Database Limits 9-6
9.2 Configuring the Security Database 9-7
9.3 Modifying the Security Database 9-9
9.4 Resetting the Security Database 9-9
9.5 Managing Security Sets 9-10
9.5.1 Create a Security Set 9-10
9.5.2 Delete a Security Set 9-10
9.5.3 Rename a Security Set 9-10
9.5.4 Copy a Security Set 9-10
9.5.5 Add Groups to a Security Set 9-11
9.5.6 Remove Groups from a Security Set 9-11
9.5.7 Activate a Security Set 9-11
9.5.8 Deactivate a Security Set 9-11
9.6 Managing Groups 9-12
9.6.1 Create a Group 9-12
9.6.2 Delete a Group 9-12
9.6.3 Rename a Group 9-12
9.6.4 Copy a Group 9-13
9.6.5 Add Members to a Group 9-13
9.6.6 Modify a Group Member 9-14
9.6.7 Remove Members from a Group 9-14

Section 10 RADIUS Server Configuration

10.1 Displaying RADIUS Server Information 10-2
10.2 Configuring a RADIUS Server on the Switch 10-3

Section 11 Event Log Configuration

11.1 Starting and Stopping Event Logging 11-1
11.2 Displaying the Event Log 11-2
11.2.1 Filtering the Event Log Display 11-3
11.2.2 Controlling Messages in the Output Stream 11-3
11.3 Managing the Event Log Configuration 11-4
11.3.1 Configure the Event Log 11-4
11.3.2 Display the Event Log Configuration 11-5
11.3.3 Restore the Event Log Configuration 11-5
11.4 Clearing the Event Log 11-5
11.5 Logging to a Remote Host 11-6
11.6 Creating and Downloading a Log File 11-7

Section 12 Simple Network Management Protocol Configuration

12.1 Managing the SNMP Service 12-1
12.2 Displaying SNMP Information 12-3
12.3 Modifying the SNMP Configuration 12-4
12.4 Resetting the SNMP Configuration 12-5

Section 13 Command Reference

13.1 Access Authority 13-1
13.2 Syntax and Keywords 13-2
13.3 Notes and Examples 13-2
13.4 Command Listing 13-3
Admin 13-4
Alias 13-5
Config 13-7
Create 13-10
Date 13-13
Exit 13-14
Fcping 13-15
Fctrace 13-16
Feature 13-18
Firmware Install 13-20
Group 13-22
Hardreset 13-30
Help 13-31
History 13-32
Hotreset 13-33
Image 13-34

Lip 13-37
Logout 13-38
Passwd 13-39
Ping 13-40
Ps 13-41
Quit 13-42
Reset 13-43
Security 13-52
Securityset 13-56
Set Alarm 13-59
Set Beacon 13-60
Set Config Port 13-61
Set Config Security 13-67
Set Config Security Portbinding 13-69
Set Config Switch 13-70
Set Config Threshold 13-72
Set Config Zoning 13-74
Set Log 13-76
Set Pagebreak 13-80
Set Port 13-82
Set Setup Radius 13-84
Set Setup Services 13-87
Set Setup SNMP 13-90
Set Setup System 13-93
Set Switch State 13-95
Set Timezone 13-96
Show About 13-97
Show Alarm 13-98
Show Broadcast 13-99
Show Chassis 13-100
Show Config Port 13-101
Show Config Security 13-103
Show Config Security Portbinding 13-104
Show Config Switch 13-105
Show Config Threshold 13-106
Show Config Zoning 13-107
Show Domains 13-108
Show Donor 13-109
Show Fabric 13-110

Show FDMI 13-111
Show Interface. 13-113
Show Log. 13-114
Show LSDB 13-117
Show Media. 13-118
Show Mem. 13-122
Show NS 13-123
Show Pagebreak 13-125
Show Perf 13-126
Show Port 13-129
Show Post Log 13-134
Show Setup Mfg 13-135
Show Setup Radius. 13-136
Show Setup Services 13-137
Show Setup SNMP 13-138
Show Setup System 13-139
Show Steering 13-140
Show Switch 13-141
Show Timezone. 13-143
Show Topology 13-144
Show Users 13-146
Show Version. 13-147
Shutdown 13-148
Test Cancel 13-149
Test Port 13-150
Test Status. 13-153
Uptime 13-154
User 13-155
Whoami 13-158
Zone 13-159
Zoneset 13-163
Zoning 13-166

Index

List of Tables

Table		Page
2-1	Command-Line Completion	2-3
3-1	Factory User Accounts	3-1
5-1	Heartbeat LED Activity	5-7
5-2	Switch Reset Methods	5-20
13-1	ISL Group Member Attributes	13-23
13-2	Port Group Member Attributes	13-24
13-3	MS Group Member Attributes	13-25
13-4	Group Member Attributes	13-26
13-5	Switch Configuration Defaults	13-46
13-6	Port Configuration Defaults	13-47
13-7	Port Threshold Alarm Configuration Defaults	13-48
13-8	Zoning Configuration Defaults	13-49
13-9	SNMP Configuration Defaults	13-49
13-10	RADIUS Configuration Defaults	13-50
13-11	Services Configuration Defaults	13-50
13-12	System Configuration Defaults	13-51
13-13	Security Configuration Defaults	13-51
13-14	Port Configuration Parameters	13-61
13-15	Security Configuration Parameters	13-67
13-16	Port Binding Configuration Parameters	13-69
13-17	Switch Configuration Parameters	13-70
13-18	Port Alarm Threshold Parameters	13-72
13-19	Zoning Configuration Parameters	13-74
13-20	RADIUS Service Settings	13-84
13-21	Switch Services Settings	13-87
13-22	SNMP Configuration Settings	13-90
13-23	System Configuration Settings	13-93
13-24	Log Monitoring Components	13-114
13-25	Transceiver Information	13-118
13-26	Show Port Parameters	13-129
13-27	Switch Operational Parameters	13-141
13-28	Port Test Parameters	13-151
13-29	Zoning Database Limits	13-167

Section 1
Introduction

This guide describes the features and use of the command line interface for SANbox 5000 Series switches running firmware version 6.7. This guide is organized as follows:

- Section 1 describes switch models and features, the intended audience, related materials, new items in this release, and technical support.
- Section 2 describes logging on and off of a switch, opening and closing an Admin session, entering commands, getting help, paging a switch, setting page breaks, and loading and retrieving files.
- Section 3 describes the management of user accounts and passwords.
- Section 4 describes configuring the switch network connection.
- Section 5 describes managing the switch configuration, setting the date and time, backing up and restoring the switch configuration, resetting the switch, installing firmware, and installing feature licenses.
- Section 6 describes port configurations, resetting a port, initializing a port loop, configuring port threshold alarms, and testing ports.
- Section 7 describes managing the zoning database and configuring interoperability.
- Section 8 describes managing connection security.
- Section 9 describes managing device security.
- Section 10 describes managing the Remote Authentication Dial-In User Service (RADIUS) server.
- Section 11 describes events and event logging.
- Section 12 describes managing the Simple Network Management Protocol (SNMP) configuration.
- Section 13 lists the commands in alphabetical order, including the command syntax, keywords, notes, and examples.

An index and a glossary are also provided.

1.1 Switch Models and Examples

The commands and displays of the command line interface vary depending on the switch model. All examples in this guide are taken from a SANbox 5600 switch unless stated otherwise.

1.2 Intended Audience

This guide is intended for individuals who are responsible for installing and servicing Fibre Channel equipment using the command line interface.

1.3 Related Materials

The following manuals and materials are referenced in the text and/or provide additional information.

- *SANbox 5000 Series Fibre Channel Switch Installation Guide,* 59096-04
- *SANbox 5000 Series QuickTools Switch Management User Guide*, 59235-01
- *SANbox 5000 Series Enterprise Fabric Suite 2007 User Guide,* 59097-04
- *SANbox Simple Network Management Protocol Reference Guide*, publication number 59047-07
- *CIM Agent Reference Guide,* 59223-01
- *SANbox CLI Quick Reference Guide*, 59261-00
- *QLogic Switch Interoperability Guide v3.0*. This PDF document can be downloaded at http://www.qlogic.com/interopguide/info.asp#inter.
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 7.0.
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
Fax: (303) 397-2740.

1.4 New in This Release

The following features are new in this release:

- The switch is equipped with the QuickTools embedded graphical user interface. QuickTools is a web applet that provides basic fabric management tools.
- The following optional features are available with the purchase and installation of a license key:
  - Enterprise Fabric Suite 2007 is a workstation-based Java® application that provides a graphical user interface for fabric management. This includes Performance View which graphs port performance. Enterprise Fabric Suite 2007 comes with a free 30-day trial license.
  - Fabric Security provides for Secure Socket Layer (SSL) and Secure Shell (SSH) connection security, device security using Challenge Handshake Authentication Protocol (CHAP), and remote authentication using a Remote Authentication Dial-In User Service (RADIUS) server.
  - SANdoctor provides tools for Fibre Channel connection verification (Fcping command), Fibre Channel route tracing (Fctrace command), and transceiver diagnostic information (Show Media command).
  - Port Activation enables additional Fibre Channel ports up to the 20-port maximum.
- You can download firmware image files using Trivial File Transfer Protocol (TFTP) using the Firmware Install, Image Install, and Image TFTP commands.
- The Zoning Delete Orphans command removes inactive zone sets and all zones and aliases not in the active zone set.
- Implicit hard zoning enforces soft zone boundaries effectively converting them to hard zones.
- Port binding establishes a list of port/devices that are permitted to log in to a switch port. Port binding is configured using the Set Config Security Portbinding command.

1.5 Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

1.5.1 Availability

QLogic Technical Support for products under warranty is available during local standard working hours excluding QLogic Observed Holidays.

1.5.2 Training

QLogic offers certification training for the technical professional for both the SANblade™ HBAs and the SANbox switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com.

1.5.3
Contact Information

Support Headquarters	QLogic Corporation 12984 Valley View Road Eden Prairie, MN 55344-3657 USA
QLogic Web Site	www.qlogic.com
Technical Support Web Site	support.qlogic.com
Technical Support Email	support@qlogic.com
Technical Training Email	tech.training@qlogic.com
North American Region	
Email	support@qlogic.com
Phone	+1-952-932-4040
Fax	+1 952-974-4910
Europe, Middle East, and Africa Region	
Email	emeasupport@qlogic.com
Phone Numbers by Language	+353 1 6924960 - English +353 1 6924961 - Français +353 1 6924962 - Deutsch +353 1 6924963 - Español +353 1 6924964 - Português +353 1 6924965 - Italiano
Asia Pacific Region	
Email	apacsupport@qlogic.com
Phone Numbers by Language	+63-2-885-6712 - English +63-2-885-6713 - (Mandarin) +63-2-885-6714 - (Japanese) +63-2-885-6715 - (Korean)
Latin and South America Region	
Email	calasupport@qlogic.com
Phone Numbers by Language	+52 55 5278 7016 - English +52 55 5278 7017 - Español +52 55 5278 7015 - Português

Notes

Section 2

Command Line Interface Usage

This section describes the following tasks:

- Logging In to the Switch
- Opening and Closing an Admin Session
- Entering Commands
- Getting Help
- Setting Page Breaks
- Creating a Support File
- Downloading and Uploading Files

NOTE: Throughout this document, references in text to commands and keywords use initial capitalization for clarity. Actual command and keyword entries are case insensitive

2.1 Logging In to the Switch

To log in to a switch through Telnet, open a command line window on the workstation and enter the Telnet command followed by the switch IP address:

```
# telnet ip_address
```

The Telnet window opens prompting you for a login. Enter an account name and password. The default account name is *admin*, and its password is *password*.

```
switch login:admin
password: xxxxxxxx

Warning:  Your user account password has not been changed
          It is strongly recommended that you do so before
          proceeding
```

To log off, enter the Exit command:

```
SANbox #> exit
```

To log in to a switch through the serial port, configure the workstation port with the following settings:

- 9600 baud
- 8-bit character
- 1 stop bit
- No parity

Enter an account name and password when prompted.

NOTE: A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for Enterprise Fabric Suite 2007 inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

2.2 Opening and Closing an Admin Session

The command line interface performs monitoring and configuration tasks. Commands that perform monitoring tasks are available to all user accounts. Commands that perform configuration tasks are available only after entering the Admin Start command to open an Admin session. A user account must have Admin authority to enter the Admin Start command.

The following is an example of how to open and close an Admin session:

```
SANbox #> admin start
SANbox (admin) #>
.
.
.
SANbox (admin) #> admin end
```

2.3 Entering Commands

The command-line completion feature makes entering and repeating commands easier. Table 2-1 describes the command-line completion keystrokes.

Table 2-1. Command-Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.
Control-U	Clears the command line.

2.4 Getting Help

To display help for a command, enter the Help command followed by the command. The following is an example of the help that is available for the Config Edit command.

```
SANbox #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

2.5 Setting Page Breaks

Some display commands deliver so much information to the screen that it scrolls off too quickly to read it. You can limit the display to 20 lines by turning on page breaks. By default, page breaks are turned off.The following is an example of how to turn page breaks on and how it affects the display.

```
SANbox #> set pagebreak on
SANbox #> zone list

  Zone        ZoneSet
  ----        -------
  Zone1
              alpha
              beta

  Zone2
              delta
              echo

  Zone3
              sierra
              tango

  Zone4
              gamma
              delta

         Press any key to continue, 'q' to quit ...
```

2.6 Creating a Support File

If you contact technical support about a problem with your switch, they may request that you create and send a support file. This support file contains all of the switch configuration information which can be helpful in diagnosing the problem. The Create Support command creates the support file (dump_support.tgz) on the switch. If your workstation has an FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation.

NOTE: Support files are deleted from the switch during a power cycle or switch reset.

The following example creates a support file and sends it to a remote host.

```
SANbox #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): y
Enter IP Address of remote computer: 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
Would you like to continue downloading support file? (y/n) [n]: y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password:  xxxxxxx

230 User johndoe logged in.
cd bin/support
250 CWD command successful.
lcd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

If your workstation does not have an FTP server, enter the Create Support command to create the support file, and use FTP to download the support file from the switch to your workstation as shown in the following example:

```
SANbox #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n
```

To download the support file from the switch to the workstation, do the following:

1. Open a terminal window and move to the directory where you want to download the support file.
2. Enter the FTP command and the switch IP address or symbolic name.

   ```
   >ftp 10.0.0.1
   ```

3. When prompted for a user and password, enter the FTP account name and password (images, images).

   ```
   user: images
   password: images
   ```

4. Set binary mode and use the Get command to download the file (dump_support.tgz).

   ```
   ftp>bin
   ftp>get dump_support.tgz
       xxxxx bytes sent in xx secs.
   ftp>quit
   ```

2.7 Downloading and Uploading Files

There are several files that reside on the switch that you can download to the workstation for examination or for safekeeping. These files include the following:

- Backup configuration file (configdata)
- Log files (logfile)
- Support files (dump_support.tgz)

You can upload firmware image files or backup configuration files to the switch to reinstall firmware or restore a corrupted configuration. The switch uses FTP to exchange files between the switch and the workstation.

- Refer to “Installing Firmware” on page 5-20 for information about installing firmware.
- Refer to “Back Up and Restore a Switch Configuration” on page 5-14 for information about backing up and restoring a switch configuration.
- Refer to “Creating and Downloading a Log File” on page 11-7 for information about creating a log file.
- Refer to “Creating a Support File” on page 2-5 for information about creating a support file.

To download a file from the switch to the workstation, do the following:

1. Enter the FTP command and the switch IP address or symbolic name.

   ```
   >ftp 10.0.0.1
   ```

2. When prompted for a user and password, enter the FTP account name and password (images, images).

   ```
   user: images
   password: images
   ```

3. Set binary mode and use the Get command to download the file (configdata).

   ```
   ftp>bin
   ftp>get configdata
       xxxxx bytes sent in xx secs.
   ftp>quit
   ```

To upload a file from the workstation to the switch, do the following

1. Enter the FTP command and the switch IP address or symbolic name.

   ```
   >ftp 10.0.0.1
   ```

2. When prompted for a user and password, enter the FTP account name and password (images, images).

   ```
   user:images
   password: images
   ```

3. Set binary mode and use the Put command to upload the file (config_switch_169).

   ```
   ftp>put config_switch_169 configdata
       xxxxx bytes sent in xx secs.
   ftp>quit
   ```

Section 3
User Account Configuration

User accounts and their respective passwords are the first line of switch security. A user account consists of an account name, an authority level, and an expiration date. Switches come from the factory with certain user accounts defined for special purposes. Table 3-1 describes these accounts, their passwords, and their purposes. These accounts cannot be deleted from the switch.

Table 3-1. Factory User Accounts

User Account Name	Password	Purpose
admin	password	This user account provides access to the Telnet server for managing the switch. Admin is the only account name that has permission to create and modify other user accounts. To secure your admin user account, be sure to change the password for this account.
images	images	This user account provides access to the File Transfer Protocol (FTP) server for exchanging files between the switch and the workstation.
prom	prom	This user account provides access to the Maintenance menu while in Maintenance mode to perform switch recovery tasks. Refer to the *SANbox 5000 Series Fibre Channel Switch Installation Guide* for information about using Maintenance mode.

This section describes the following user account configuration tasks:

- Displaying User Account Information
- Creating User Accounts
- Modifying User Accounts and Passwords

3.1 Displaying User Account Information

You can display all user accounts defined on the switch (User Accounts command) or just those user accounts that are logged on (User List or Show Users commands).

The following example displays all user accounts defined on the switch. Account information includes account name, authority, and expiration date.

```
SANbox (admin) #> user accounts

  Current list of user accounts
-----------------------------
images       (admin authority = False, never expires)
admin        (admin authority = True , never expires)
chuckca      (admin authority = False, expires in < 50 days)
gregj        (admin authority = True , expires in < 100 days)
fred         (admin authority = True , never expires)
```

The following example displays user accounts that are logged on to the switch:

```
SANbox (admin) #> user list

User                        Ethernet Addr-Port    Logged in Since
----                        ------------------    ---------------
admin@OB-session1           10.20.68.108-1031     day month date time year
admin@OB-session2           10.20.68.108-1034     day month date time year
snmp@OB-session3            Unknown               day month date time year
snmp@IB-session4            Unknown               day month date time year
admin@OB-session5           Unknown               day month date time year
```

3.2 Creating User Accounts

A user account consists of an account name, an authority level, and an expiration date. The account name can be up to 15 characters and must begin with an alphanumeric character. The authority level grants admin authority (true) or denies it (false). The expiration date sets the date when the user account expires. Only the Admin user account can create user accounts.

The following example creates a new user account named user1 with admin authority that expires in 100 days.

```
SANbox (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

3.3 Modifying User Accounts and Passwords

Only the Admin user account can modify a user account, delete a user account, or change the password of another user account. However, all user accounts can change their own passwords. The User command modifies and deletes user accounts. The Passwd command changes passwords.

The following example removes the expiration date and admin authority for the user account named user1.

```
SANbox (admin) #> user edit

     Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following example deletes the user account named user3.

```
SANbox (admin) #> user delete user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

In the following example, the Admin user account changes the password for the user account named user2.

```
SANbox #> admin start
SANbox (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (8-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Section 4

Network and Fabric Configuration

The switch network configuration consists of the following:

- Network discovery method
- IP address
- Subnet mask
- IP gateway address

The network discovery method determines how the switch acquires its IP address. The IP address can come from the IP address that resides on the switch or from a server. The switch supports network discovery from the following server types:

- Bootstrap Protocol (BootP)
- Reverse Address Resolution Protocol (RARP)
- Dynamic Host Configuration Protocol (DHCP)

This section describes the following network configuration tasks:

- Displaying Name Server Information
- Displaying the Ethernet Network Configuration
- Configuring the Ethernet Port
- Verifying a Switch in the Network

4.1 Displaying Name Server Information

The Show NS command displays the list of WWNs in fabric as shown in the following example:

```
SANbox #> show ns all
 Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 1.

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 4.

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   8 (0x8)   0824ba NL   3   22:00:00:20:37:2b:08:00 20:00:00:20:37:2b:08:00
  2   8 (0x8)   0824c3 NL   3   22:00:00:20:37:2b:08:78 20:00:00:20:37:2b:08:78
  3   8 (0x8)   0824c5 NL   3   22:00:00:20:37:1b:cf:fd 20:00:00:20:37:1b:cf:fd
  4   8 (0x8)   0824c6 NL   3   22:00:00:20:37:2b:07:b4 20:00:00:20:37:2b:07:b4
  5   8 (0x8)   0824c9 NL   3   22:00:00:20:37:2b:08:57 20:00:00:20:37:2b:08:57
  6   8 (0x8)   0824cb NL   3   22:00:00:20:37:1b:cf:f6 20:00:00:20:37:1b:cf:f6
  7   8 (0x8)   0824cc NL   3   22:00:00:20:37:2b:0b:ec 20:00:00:20:37:2b:0b:ec
  8   8 (0x8)   0824d6 NL   3   22:00:00:20:37:2b:07:e1 20:00:00:20:37:2b:07:e1
  9   8 (0x8)   0824da NL   3   22:00:00:20:37:2b:0b:1a 20:00:00:20:37:2b:0b:1a
  10  8 (0x8)   0824e0 NL   3   22:00:00:20:37:1b:f0:7d 20:00:00:20:37:1b:f0:7d
  11  8 (0x8)   0824e1 NL   3   22:00:00:20:37:2b:02:f6 20:00:00:20:37:2b:02:f6
  12  8 (0x8)   0824e2 NL   3   22:00:00:20:37:1b:ea:b7 20:00:00:20:37:1b:ea:b7
  13  8 (0x8)   0824e8 NL   3   22:00:00:20:37:1b:cb:e5 20:00:00:20:37:1b:cb:e5

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 10.

  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  No entries found for domain ID 34.
```

4.2 Displaying the Ethernet Network Configuration

The Show Fabric command displays IP addresses (Enet IP Addr) for all switches in the fabric as shown in the following example.

```
SANbox #> show fabric
 Domain     WWN                     Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                     ------------    ----------      ------------
 16 (0x10)  10:00:00:c0:dd:00:77:81 10.20.68.11     0.0.0.0         gui sb1 .11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d 10.20.68.12     0.0.0.0         sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 10.20.68.160    0.0.0.0         sw .160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 10.20.68.108    0.0.0.0         Sb2 .108
```

The Show Setup System command displays the switch network configuration as shown in the following example:

```
SANbox #> show setup system
  System Information
  ------------------
  EthNetworkEnable         True
  EthNetworkDiscovery      Static
  EthNetworkAddress        10.20.11.32
  EthNetworkMask           255.255.252.0
  EthGatewayAddress        10.20.8.254
  AdminTimeout             30
  InactivityTimeout        0
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
  NTPClientEnabled         True
  NTPServerAddress         51.68.85.102
  EmbeddedGUIEnabled       True
```

4.3 Configuring the Ethernet Port

Configure the switch Ethernet port using the Set Setup System command within an Admin session. The following example configures a new IP address, subnet mask, and gateway address.

```
SANbox (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

EthNetworkDiscovery     (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
EthNetworkAddress       (dot-notated IP Address)             [10.0.0.1     ] 10.20.30.40
EthNetworkMask          (dot-notated IP Address)             [255.255.255.0] 255.0.0.0
EthGatewayAddress       (dot-notated IP Address)            [10.0.0.254   ] 10.20.30.254
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
InactivityTimeout       (dec value 0-1440 minutes, 0=never)  [0            ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
NTPClientEnabled        (True / False)                       [False        ]
NTPServerAddress        (dot-notated IP Address)             [10.0.0.254   ]
EmbeddedGUIEnabled      (True / False)                       [True         ]

  Do you want to save and activate this system setup? (y/n): [n] y
```

4.4 Verifying a Switch in the Network

You can verify that a switch is communicating in the network using the Ping command. The following example successfully tests the network for a switch with IP address 10.20.11.57.

```
SANbox #> ping 10.20.11.57
  Ping command issued. Waiting for response...
SANbox #>
  Response successfully received from 10.20.11.57.
```

If the switch was unreachable, you would see the following display.

```
SANbox #> ping 10.20.11.57
  Ping command issued. Waiting for response...
  No response from 10.20.11.57. Unreachable.
```

4.5 Verifying and Tracing Fibre Channel Connections

NOTE: The Fcping and Fctrace commands require the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller.

You can verify Fibre Channel connections between the switch and the fabric and display routing information. Enter the Fcping command to verify a Fibre Channel connection to a switch or a device as shown in the following example. The target device can be defined as a Fibre Channel address or a WWN.

```
SANbox #> fcping 970400 count 3
28 bytes from local switch to 0x970400 time = 10 usec
28 bytes from local switch to 0x970400 time = 11 usec
28 bytes from local switch to 0x970400 time = 119 usec
```

The following is an example of a connection failure:

```
SANbox #> fcping 0x113344 count 3
     28 bytes from local switch to 0x113344 failed
```

Enter the Fctrace command to display Fibre Channel routing information between two devices as shown in the following example. The devices can be defined as Fibre Channel addresses or WWNs.

```
SANbox#> fctrace 970400 970e00 hops 5

  36 bytes from 0x970400 to 0x970e00, 5 hops max

  Domain  Ingress Port WWN         Port  Egress Port WWN          Port
  ------  ----------------         ----  ---------------          ----
  97      20:04:00:c0:dd:02:cc:2e  4     20:0e:00:c0:dd:02:cc:2e  14
  97      20:0e:00:c0:dd:02:cc:2e  14    20:04:00:c0:dd:02:cc:2e  4
```

Section 5

Switch Configuration

Switch configuration consists of the following tasks:

- Displaying Switch Information
- Managing Switch Services
- Managing Switch Configurations
- Paging a Switch
- Setting the Date and Time
- Resetting a Switch
- Installing Firmware
- Managing Switch Feature Upgrades

5.1 Displaying Switch Information

You can display the following types of the switch information:

- Switch Operational Information
- System Process Information
- Elapsed Time Between Resets
- Configuration Information
- Hardware Information
- Firmware Information

5.1.1
Switch Operational Information

The Show Switch command displays a variety of switch operational information. These include the switch WWN, domain ID, firmware version, administrative state, and operational state as shown in the following example:

```
SANbox #> show switch
  Switch Information
  ------------------
  SymbolicName                     SANbox
  SwitchWWN                        10:00:00:c0:dd:00:bc:56
  BootVersion                      Vx.x.x.x-0 (day month date time year)
  CreditPool                       0
  DomainID                         19 (0x13)
  FirstPortAddress                 130000
  FlashSize - MBytes               128
  LogFilterLevel                   Critical
  MaxPorts                         20
  NumberOfSwitchResets             15
  ReasonForLastReset               PowerUp
  ActiveImageVersion - build date  Vx.x.x.0 (day month date time year)
  PendingImageVersion - build date Vx.x.x.0 (day month date time year)
  ActiveConfiguration              default
  AdminState                       Online
  AdminModeActive                  False
  Beacon                           Off
  OperationalState                 Online
  PrincipalSwitchRole              False
  BoardTemp (1) - Degrees Celsius  32
  SwitchDiagnosticsStatus          Passed
  SwitchTemperatureStatus          Normal
```

5.1.2
System Process Information

The Ps command displays system process information to help you determine what processes are running and CPU usage. The following example displays current system processes.

```
SANbox #> ps
PID  PPID %CPU     TIME     ELAPSED COMMAND
338   327  0.0 00:00:00  3-01:18:35 cns
339   327  0.0 00:00:01  3-01:18:35 ens
340   327  0.0 00:00:21  3-01:18:35 dlog
341   327  0.1 00:05:35  3-01:18:35 ds
342   327  0.2 00:11:29  3-01:18:35 mgmtApp
343   327  0.0 00:00:04  3-01:18:35 fc2
344   327  0.0 00:02:16  3-01:18:35 nserver
345   327  0.0 00:02:44  3-01:18:35 mserver
346   327  0.8 00:35:12  3-01:18:35 util
347   327  0.0 00:00:29  3-01:18:35 snmpservicepath
348   327  0.0 00:02:46  3-01:18:34 eport
349   327  0.0 00:00:21  3-01:18:34 PortApp
350   327  5.6 04:08:24  3-01:18:34 port_mon
351   327  0.0 00:01:38  3-01:18:34 zoning
352   327  0.0 00:00:01  3-01:18:34 diagApp
404   327  0.0 00:00:04  3-01:18:27 snmpd
405   327  0.0 00:00:02  3-01:18:27 snmpmain
406   405  0.0 00:00:00  3-01:18:26 snmpmain
```

The column titles are as follows:

- PID–Process identifier
- PPID–Parent process identifier
- %CPU–Percentage CPU usage
- TIME–Actual processing time
- ELAPSED–Elapsed time since the process started
- COMMAND–The command that initiated the process.

5.1.3
Elapsed Time Between Resets

The Uptime command displays the elapsed time since the switch was last reset and the reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed time reported by this command. The following example displays the time since the last reset.

```
SANbox #> uptime
  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

5.1.4
Configuration Information

The Show Config command displays a variety of configuration information at the port and switch levels. In addition to the basic switch configurations, the Show Config command displays parameters that control how data is maintained in the security and zoning databases. The Show Config command displays the following types of information:

- Switch Configuration Parameters
- Zoning Configuration Parameters
- Security Configuration Parameters

Refer to "Displaying Port Information" on page 6-1 for information about displaying port configuration information.

5.1.4.1
Switch Configuration Parameters

Enter the Show Config Switch command to display the switch configuration parameters. These parameters determine the operational characteristics of the switch. Refer to Table 13-17 for a description these parameters.

```
SANbox #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DefaultDomainID       19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

5.1.4.2
Zoning Configuration Parameters

Enter the Show Config Zoning command to display zoning configuration parameters. These parameters determine how zoning is applied to the switch. Refer to Table 13-19 for a description of these parameters.

```
SANbox #> show config zoning

 Configuration Name: default
  -------------------

  Zoning Configuration Information
  --------------------------------
  InteropAutoSave       True
  DefaultZone           True
  DiscardInactive       False
```

5.1.4.3
Security Configuration Parameters

Enter the Show Config Security command to display security configuration and port binding parameters. These parameters determine how security is applied to the switch. Refer to Table 13-15 for a description of the switch security configuration parameters. Refer to Table 13-16 for a description of the port binding parameters.

```
SANbox #> show config security

  Configuration Name: default
  -------------------

  Switch Security Configuration Information
  -----------------------------------------
  FabricBindingEnabled  False
  AutoSave              True

  Port  Binding Status  WWN
  ----  --------------  ---
  0     Enabled         10:00:00:00:00:00:00:01
  2     Disabled        10:00:00:00:00:00:00:01
  5     Enabled         10:00:00:00:00:00:00:01
                        10:00:00:00:00:00:00:02
```

5.1.5
Hardware Information

Enter the Show Chassis command to display the status of the switch hardware including fans, power supplies, internal temperature, and Heartbeat LED status.

The following is an example of the Show Chassis command for model 5602:

```
SANbox #> show chassis
   Chassis Information
  ------------------
  BoardTemp (1) - Degrees Celsius   36
  FanStatus (1)                     Good
  FanStatus (2)                     Good
  FanDirection (1)                  BackToFront
  FanDirection (2)                  BackToFront
  PowerSupplyStatus (1)             Good
  PowerSupplyStatus (2)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

The HeartBeatCode and HeartBeatStatus entries indicate the Power-on Self Test (POST) results revealed by the Heartbeat LED blink patterns. The result is normal operation or a blink pattern indicating a critical error as described in Table 5-1. Refer to your *Installation Guide* for more information about the Heartbeat LED and its blink patterns.

Table 5-1. Heartbeat LED Activity

HeartBeatCode–HeartBeatStatus	Description
1–Normal	One blink per second–Normal operation
2–AppDied	Two blink cluster–Internal firmware failure
3–PostFailed	Three blink cluster–Fatal POST error
4–CorruptFilesystem	Four blink cluster–Configuration file system error
5–Overheating	Five blink cluster– Over temperature

5.1.6
Firmware Information

Enter the Show Version command to display a summary of switch identity information including the firmware version. The following is an example of the Show Version command:

```
SANbox #> show version
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription     SANbox 5000 FC Switch
       EthNetworkAddress     10.20.11.192 (use 'set setup system' to update)
       EthMACAddress         00:c0:dd:00:71:ee
       WorldWideName         10:00:00:c0:dd:00:71:ed
       ChassisSerialNumber   FAM033100024
       SymbolicName          SANbox
       ActiveSWVersion       V6.7.x.x.xx.xx
       ActiveTimestamp       day month date time year
       DiagnosticsStatus     Passed
       LicensedPorts         20
```

5.2 Managing Switch Services

You can configure your switch to suit the demands of your environment by enabling or disabling a variety of switch services. You manage the switch services using the Show Setup Services and Set Setup Services commands. Refer to Table 13-21 for a description of the switch services.

NOTE: The SSH and SSL services require the Fabric Security license key.

Enter the Show Setup Services command to display the current switch service status as shown in the following example:

```
SANbox #> show setup services
System Services
----------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLEnabled                False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
MgmtServerEnabled         True
```

Enter the Set Setup Services command within an Admin session to configure the switch services as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> set setup services

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False]
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False]
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]

  Do you want to save and activate this services setup? (y/n): [n]
```

5.3 Managing Switch Configurations

The switch configuration determines the basic operational characteristics of the switch. A switch supports up to 10 configurations including the default configuration, named Default Config. The current switch operating characteristics are determined by the active configuration. Only one configuration can be active at one time.

Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components. Managing Switch Configurations describes the following tasks:

- Display a List of Switch Configurations
- Activate a Switch Configuration
- Copy a Switch Configuration
- Delete a Switch Configuration
- Modify a Switch Configuration
- Back Up and Restore a Switch Configuration

5.3.1 Display a List of Switch Configurations

Enter the Config List command to display the configurations stored on the switch as show in the following example. Notice that the Config List command does not require an Admin session.

```
SANbox #> config list

  Current list of configurations
  ------------------------------
  default
  config_1
  config_2
```

5.3.2 Activate a Switch Configuration

Enter the Config Activate command to activate a switch configuration (config_1) as shown in the following example:

```
SANbox (admin) config activate config_1
```

5.3.3
Copy a Switch Configuration

Enter the Config Copy command to create a copy of an existing configuration as shown in the following example:

```
SANbox (admin) config copy config_1 config_2
```

5.3.4
Delete a Switch Configuration

Enter the Config Delete command to delete a configuration from the switch as shown in the following example. You cannot delete the active configuration nor the default configuration (Default Config).

```
SANbox (admin) config delete config_2
```

5.3.5
Modify a Switch Configuration

To modify a switch configuration, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through Telnet, Enterprise Fabric Suite 2007, or another management application. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed.

The Config Edit session provides access to the Set Config commands with which you make modifications to the port, switch, port threshold alarm, or zoning configuration components as shown:

```
SANbox #> admin start
SANbox (admin) #> config edit
   The config named default is being edited.
SANbox (admin-config)#> set config port . . .
SANbox (admin-config)#> set config switch . . .
SANbox (admin-config)#> set config threshold . . .
SANbox (admin-config)#> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named *Default* are being saved to a new configuration named *config_10132003*. However, the new configuration does not take effect until you activate it with the Config Activate command:

```
SANbox (admin-config)#> config save config_10132003
SANbox (admin)#> config activate config_10132003
SANbox (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

The following is an example of the Set Config Switch command. Refer to Table 13-17 for a description of the switch configuration parameters.

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState          (1=Online, 2=Offline, 3=Diagnostics)   [Online        ]
  BroadcastEnabled    (True / False)                         [True          ]
  InbandEnabled       (True / False)                         [True          ]
  FDMIEnabled         (True / False)                         [True          ]
  FDMIEntries         (decimal value, 0-1000)                [1000          ]
  DefaultDomainID     (decimal value, 1-239)                 [2             ]
  DomainIDLock        (True / False)                         [False         ]
  SymbolicName        (string, max=32 chars)                 [SANbox        ]
  R_A_TOV             (decimal value, 100-100000 msec)       [10000         ]
  E_D_TOV             (decimal value, 10-20000 msec)         [2000          ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]
  InteropMode         (0=Standard, 1=Interop_1)              [Standard      ]
```

To make temporary changes to the switch administrative state, enter the Set Switch State command.

5.3.6
Back Up and Restore a Switch Configuration

Successful management of switches and fabrics depends on the effective use of switch configurations. Backing up and restoring a configuration is useful to protect your work or for use as a template in configuring other switches. Backing up and restoring the switch configuration involves the following:

- Creating the Backup File
- Downloading the Configuration File
- Restoring the Configuration File

5.3.6.1
Creating the Backup File

The Config Backup command creates a file on the switch, named *configdata*. This file can be used to restore a switch configuration only from the command line interface; it cannot be used to restore a switch using Enterprise Fabric Suite 2007.

```
SANbox #> config backup
```

The *configdata* file contains the following switch configuration information:

- All named switch configurations including port, switch, port threshold alarm, and zoning configurations components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database includes all zone sets, zones, and aliases.
- The security database except the group primary and secondary secrets.

NOTE: Configuration backup files are deleted from the switch during a power cycle, switch reset, or a transfer of the primary role to the secondary CPU blade.

5.3.6.2

Downloading the Configuration File

You use FTP to download the *configdata* file to your workstation for safe keeping and to upload the file back to the switch for the restore function. To download the configdata file, open an FTP session on the switch and login with the account name *images* and password *images*. Transfer the file in binary mode with the Get command as shown in the following example:

```
>ftp ip_address
user:images
password: images
ftp>bin
ftp>get configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

You should rename the *configdata* file on your workstation with the switch name and date, *config_switch_169_10112003*, for example.

5.3.6.3

Restoring the Configuration File

The restore operation begins with FTP to upload the configuration file from the workstation to the switch, then finishes with a Telnet session and the Config Restore command. To upload the configuration file, *config_switch_169_10112003* in this case, open and FTP session with account name *images* and password *images*. Transfer the file in binary mode with the Put command as shown:

```
ftp ip_address
user: images
password: images
ftp> bin
ftp> put config_switch_169_10112003 configdata
  Local file config_switch_169_10112003
  Remote file configdata
ftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. To restore the switch, open a Telnet session (a new IP address may be required), then enter the Config Restore command from within an Admin session as shown:

```
SANbox #> admin start
SANbox (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is being
restored -  this could take several minutes]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be reset in
3 seconds due to a config restore]
SANbox (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being reset]
```

5.4 Paging a Switch

To help you locate a particular switch in a rack of switches, you can turn on the beacon feature with the Set Beacon command. This causes all port Logged-In LEDs to flash in unison. The following is an example of how to turn the beacon on and off.

```
SANbox #> set beacon on
SANbox $> set beacon off
```

5.5 Setting the Date and Time

The switch date and time can be set explicitly using the Date command or it can be set automatically through a Network Time Protocol (NTP) server. The Date command also displays the current time. Unlike the Date command, the NTP server also synchronizes the date and time on the switch with the date and time on the workstation. Synchronized date and time is required for Secure Socket Layer (SSL) connections.

You can also set the time zone using the Set Timezone command. The default time zone is Universal Time (UTC) also known as Greenwich Mean Time. Changing the time zone also converts the current time to the time in the new time zone. For this reason, if you are not using an NTP server, set the time zone first, then set the date and time.

To use an NTP server, you must enable the NTP client on the switch and specify an IP address for the NTP server.

NOTE: To set the date with the Date command, the NTP client must be disabled.

Enter the Set Timezone to change the time zone as shown in the following example:

```
SANbox (admin) #> set timezone
  Africa                                America
  Antarctica                            Asia
  Atlantic                              Australia
  Europe                                Indian
  Pacific                               UTC
        Press ENTER for more options or 'q' to make a selection.

  America/Grenada                       America/Guadeloupe
  America/Guatemala                     America/Guayaquil
  America/Guyana                        America/Halifax
  America/Havana                        America/Hermosillo
  America/Indiana                       America/Indianapolis
  .
  .
  .
  America/Monterrey                     America/Montevideo
  America/Montreal                      America/Montserrat
  America/Nassau                        America/New_York
  America/Nipigon                       America/Nome
  America/Noronha                       America/North_Dakota
  America/Panama                        America/Pangnirtung

        Press ENTER for more options or 'q' to make a selection.
q
  Enter selection (or 'q' to quit): america/north_dakota
  America/North_Dakota/Center
  Enter selection (or 'q' to quit): america/north_dakota/center
```

Enter the Date command to display the date and time as shown in the following example:

```
SANbox #> date
  Mon Apr 07 07:51:24 200x
```

Enter the Date command within an Admin session to set the date and time as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> date 013110152025
SANbox (admin) #> date
  Fri Jan 31 10:15:03 UTC 2025
```

To configure the switch to use an NTP server, enter the Set Setup System command to enable the NTP client and to specify the NTP server IP address.

```
SANbox  #> admin start
SANbox (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

EthNetworkDiscovery  (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp) [Static       ]
EthNetworkAddress    (dot-notated IP Address)            [10.0.0.1     ]
EthNetworkMask       (dot-notated IP Address)            [255.255.255.0]
EthGatewayAddress    (dot-notated IP Address)            [10.0.0.254   ]
AdminTimeout         (dec value 0-1440 minutes, 0=never) [30           ]
InactivityTimeout    (dec value 0-1440 minutes, 0=never) [0            ]
LocalLogEnabled      (True / False)                      [True         ]
RemoteLogEnabled     (True / False)                      [False        ]
RemoteLogHostAddress (dot-notated IP Address)            [10.0.0.254   ]
NTPClientEnabled     (True / False)                      [False        ] True
NTPServerAddress     (dot-notated IP Address)            [10.0.0.254   ] 10.2.3.4
EmbeddedGUIEnabled   (True / False)                      [True         ]

Do you want to save and activate this services setup? (y/n): [n] y
System setup saved and activated.
```

5.6 Resetting a Switch

Table 5-2 describes the methods for resetting a switch, the corresponding command, and the impact on the switch.

Table 5-2. Switch Reset Methods

Description	Hot Reset (Hotreset command)	Soft Reset (Reset Switch command)	Hard Reset (Hardreset Switch command)
Activates pending firmware	✔	✔	✔
Disrupts I/O traffic		✔	✔
Enterprise Fabric Suite 2007 sessions reconnect afterwards	✔	✔	✔
Clears the event log	✔	✔	✔
Deletes supports files, firmware image files that have not been unpacked, and configuration backup files		✔	✔
Closes all management sessions	✔	✔	✔
Power-on self test			✔

5.7 Installing Firmware

New firmware becomes available periodically either on CD-ROM or from the QLogic web site. Installing firmware on a switch involves the following steps:

1. Download the firmware image file to the switch.
2. Unpack the firmware image file.
3. Activate the new firmware. The activation can be disruptive or non-disruptive. Refer to “Nondisruptive Activation” on page 5-21 for information about the conditions for a non-disruptive activation.

The Firmware Install and the Image Install commands automate the firmware installation process and perform a disruptive activation as described in “One-Step Firmware Installation” on page 5-21. To perform a nondisruptive activation, refer to “Custom Firmware Installation” on page 5-23.

5.7.1
Nondisruptive Activation

You can load and activate new firmware on a switch disruptively or nondisruptively depending on the condition of the fabric and the commands you choose. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the activation will fail. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation.

- The current firmware version permits the installation and non-disruptive activation of 6.7 firmware. Refer to the 6.7 Firmware Release Notes for previous compatible firmware versions.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, changing switch configurations, or installing firmware.
- No port on the switch is in the diagnostic state.
- No Zoning Edit sessions are open on the switch.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.
- Install firmware on one switch at a time in the fabric. If you are installing firmware on one switch, wait 120 seconds after the activation is complete before installing firmware on a second switch.
- For a fabric in which one or more switches are running firmware prior to version 6.7, only one Enterprise Fabric Suite 2007 session can be open.

Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, Enterprise Fabric Suite 2007 sessions reconnect automatically. However, Telnet sessions must be restarted manually.

5.7.2
One-Step Firmware Installation

The Firmware Install and Image Install commands download the firmware image file from an FTP or TFTP server to the switch, unpacks the image file, and performs a disruptive activation in one step. The one-step installation process prompts you to enter the following:

- The file transfer protocol (FTP or TFTP)
- IP address of the remote host
- An account name and password on the remote host (FTP only)

- Pathname for the firmware image file

1. Enter the following commands to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware.

```
SANbox #> admin start
SANbox #> firmware install
  The switch will be reset. This process will cause a
  disruption to I/O traffic.
  Continuing with this action will terminate all management
  sessions,including any Telnet sessions. When the firmware
  activation is complete, you may log in to the switch again.
  Do you want to continue? [y/n]: y
  Press 'q' and the ENTER key to abort this command.
```

2. Enter your choice for the file transfer protocol with which to download the firmware image file. FTP requires an user account and a password; TFTP does not.

```
  FTP or TFTP     : ftp
```

3. Enter your account name on the remote host (FTP only) and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

```
  User Account    : johndoe
  IP Address      : 10.0.0.254
  Source Filename : 6.7.00.11_mpc
  About to install image.  Do you want to continue? [y/n] y
```

4. When prompted to install the new firmware, enter Yes to continue or No to cancel. Entering Yes will disrupt traffic. This is the last opportunity to cancel.

```
About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).
220 localhost.localdomain FTP server (Version wu-2.6.1-18)
ready.
```

5. Enter the password for your account name (FTP only).

```
331 Password required for johndoe.
Password:******
230 User johndoe logged in.
```

6. The firmware will now be downloaded from the remote host to the switch, installed, and activated.

5.7.3
Custom Firmware Installation

A custom firmware installation downloads the firmware image file from a remote host to the switch, unpacks the image file, and resets the switch in separate steps. This allows you to choose the type of switch reset and whether the activation will be disruptive (Reset Switch command) or nondisruptive (Hotreset command). The following example illustrates a custom firmware installation with a nondisruptive activation.

1. Download the firmware image file from the workstation to the switch.
   - If your workstation has an FTP server, you can enter the Image Fetch command:

     `SANbox #> admin start`

     `SANbox (admin) #> image fetch` *`account_name ip_address filename`*
   - If your workstation has a TFTP server, you can enter the Image TFTP command to download the firmware image file.

     `SANbox (admin) #> image tftp` *`ip_address filename`*
   - If your workstation has neither an FTP nor a TFTP server, open an FTP session and download the firmware image file by entering FTP commands:

     `>ftp` *`ip_address`* `or` *`switchname`*

     `user:images`

     `password: images`

     `ftp>bin`

     `ftp>put` *`filename`*

     `ftp>quit`
2. Display the list of firmware image files on the switch to confirm that the file was loaded.

   `SANbox #> admin start`

   `SANbox (admin) $> image list`
3. Unpack the firmware image file to install the new firmware in flash memory.

   `SANbox (admin) $> image unpack` *`filename`*
4. Wait for the unpack to complete.

   `Image unpack command result: Passed`
5. A message will prompt you to reset the switch to activate the firmware. Use the Hotreset command to attempt a non-disruptive activation.

   `SANbox (admin) $> hotreset`

5.8 Managing Switch Feature Upgrades

The following features are available to upgrade your switch through the purchase and installation of a license key:

- Enterprise Fabric Suite 2007 is a workstation-based Java® application that provides a graphical user interface for fabric management. This includes Performance View which graphs port performance. Enterprise Fabric Suite 2007 comes with a free 30-day trial license.
- Fabric Security provides for Secure Socket Layer (SSL) and Secure Shell (SSH) connection security, device security using Challenge Handshake Authentication Protocol (CHAP), and remote authentication using a Remote Authentication Dial-In User Service (RADIUS) server.
- SANdoctor provides tools for Fibre Channel connection verification (Fcping command), Fibre Channel route tracing (Fctrace command), and transceiver diagnostic information (Show Media command).
- Port Activation enables additional Fibre Channel ports up to the 20-port maximum.

Installing a feature license key is not disruptive, nor does it require a switch reset. To order a license key, contact your switch distributor or your authorized reseller.

5.8.1 Display Feature Licenses

Enter the Feature Log command to display the license keys that are installed on your switch as shown in the following example:

```
SANbox #> feature log
  Mfg Feature Log:
  ----------------
  Switch Licensed for 8 ports
  Customer Feature Log:
  ---------------------
  1) day month date 19:39:24 year - Switch Licensed for 20 ports
  1-LCVXOWUNOJBE6
```

5.8.2
Install a Feature License Key

Enter the Feature Add command to install a license key on your switch as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> feature add 1-LCVXOWUNOJBE6
License upgrade to 20 ports

Do you want to continue with license upgrade procedure? (y/n): [n] y
Alarm Msg:[day mon date time year][A1005.0030][SM][Upgrading Licensed Ports to 20]
```

Notes

Section 6

Port Configuration

This section describes the following topics:

- Displaying Port Information
- Modifying Port Operating Characteristics
- Port Binding
- Resetting a Port
- Configuring Port Threshold Alarms
- Testing a Port
- Extending Port Transmission Distance

6.1 Displaying Port Information

You can display the following port information:

- Port Configuration Parameters
- Port Operational Information
- Port Threshold Alarm Configuration Parameters
- Port Performance

6.1.1
Port Configuration Parameters

Enter the Show Config Port command to display the port configuration parameters. These parameters determine the operational characteristics of the port. Refer to Table 13-14 for a description of these parameters.

```
SANbox #> show config port 3

  Configuration Name: default
  ---------------------------

  Port Number: 3
  ------------
  AdminState         Offline
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port3
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  LCFEnabled         False
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Disabled
  VIEnabled          False
  MFSEnabled         True
  PDISCPingEnable    True
```

6.1.2
Port Operational Information

Enter the Show Port command to display port operational information.

```
SANbox #> show port 1
  Port Number: 1
  ------------
  AdminState       Online              OperationalState Offline
  AsicNumber       0                   PerfTuningMode   Normal
  AsicPort         0                   PortID           220000
  ConfigType       GL                  PortWWN          20:00:00:c0:dd:07:20:58
  DiagStatus       Passed              RunningType      Unknown
  EpConnState      None                MediaPartNumber  PL-XPL-VC-SG3-22
  EpIsoReason      NotApplicable       MediaRevision    1
  IOStreamGuard    Disabled            MediaType        400-M5-SN-I
  LinkSpeed        Auto                MediaVendor      PICOLIGHT
  LinkState        Inactive            MediaVendorID    00000485
  LoginStatus      NotLoggedIn         SymbolicName     Port0
  MaxCredit        16                  SyncStatus       SyncLost
  MediaSpeeds      1Gb/s, 2Gb/s, 4Gb/s XmitterEnabled   True

  ALInit             2                   LIP_F8_F7          0
  ALInitError        0                   LinkFailures       0
  BadFrames          0                   Login              0
  BBCR_FrameFailures 0                   Logout             0
  BBCR_RRDYFailures  0                   LongFramesIn       0
  Class2FramesIn     0                   LoopTimeouts       0
  Class2FramesOut    0                   LossOfSync         0
  Class2WordsIn      0                   LostFrames         0
  Class2WordsOut     0                   LostRRDYs          0
  Class3FramesIn     0                   PrimSeqErrors      0
  Class3FramesOut    0                   RxLinkResets       0
  Class3Toss         0                   RxOfflineSeq       0
  Class3WordsIn      0                   ShortFramesIn      0
  Class3WordsOut     0                   TotalErrors        0
  DecodeErrors       0                   TotalLinkResets    0
  EpConnects         0                   TotalLIPsRecvd     0
  FBusy              0                   TotalLIPsXmitd     4
  FlowErrors         0                   TotalOfflineSeq    3
  FReject            0                   TotalRxFrames      0
  InvalidCRC         0                   TotalRxWords       0
  InvalidDestAddr    0                   TotalTxFrames      0
  LIP_AL_PD_AL_PS    0                   TotalTxWords       0
  LIP_F7_AL_PS       0                   TxLinkResets       0
  LIP_F7_F7          0                   TxOfflineSeq       3
  LIP_F8_AL_PS       0
```

6.1.3
Port Threshold Alarm Configuration Parameters

Enter the Show Config Threshold command to display the port threshold alarm parameters. These parameters determine the error thresholds at which the switch issues alarms. Refer to Table 13-18 for a description of these parameters.

```
SANbox #> show config threshold
  Configuration Name: default
  ------------
  Threshold Configuration Information
  -----------------------------------
  ThresholdMonitoringEnabled      False
  CRCErrorsMonitoringEnabled      True
    RisingTrigger                 25
    FallingTrigger                1
    SampleWindow                  10
  DecodeErrorsMonitoringEnabled   True
    RisingTrigger                 25
    FallingTrigger                0
    SampleWindow                  10
  ISLMonitoringEnabled            True
    RisingTrigger                 2
    FallingTrigger                0
    SampleWindow                  10
  LoginMonitoringEnabled          True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LogoutMonitoringEnabled         True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LOSMonitoringEnabled            True
    RisingTrigger                 100
    FallingTrigger                5
    SampleWindow                  10
```

6.1.4
Port Performance

Enter the Show Perf command to display port performance in terms of the volume of data transmitted, data received, or errors. You can display continuous live performance information for one or more ports, or an instantaneous summary. The following example displays an instantaneous summary in bytes and frames. Values are expressed in thousands (K) and millions (M) of bytes or frames per second.

```
SANbox #> show perf
```

Port Number	Bytes/s (in)	Bytes/s (out)	Bytes/s (total)	Frames/s (in)	Frames/s (out)	Frames/s (total)
0	7K	136M	136M	245	68K	68K
1	58K	0	58K	1K	0	1K
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	7K	7K	0	245	245
7	136M	58K	136M	68K	1K	70K
8	7K	136M	136M	245	68K	68K
9	58K	0	58K	1K	0	1K
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	7K	7K	0	245	245
15	136M	58K	136M	68K	1K	70K
16	47M	23K	47M	23K	726	24K
17	0	0	0	0	0	0
18	23K	47M	47M	726	23K	24K
19	0	0	0	0	0	0

6.1.5
Transceiver Information

NOTE: The Show Media command requires the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller.

Enter the Show Media command to display operational information about one or more transceivers as shown in the following example. Refer to Table 13-25 for a description of the transceiver information in the Show Media display.

```
SANbox #> show media 4
Port Number: 4
-------------
MediaType           400-M5-SN-I
MediaVendor         FINISAR CORP.
MediaPartNumber     FTRJ8524P2BNL
MediaRevision       A
MediaSerialNumber   P6G22RL
MediaSpeeds         1Gb/s, 2Gb/s, 4Gb/s

                      Temp      Voltage      Tx Bias      Tx Pwr      Rx Pwr
                       (C)          (V)         (mA)        (mW)        (mW)
               ----------- ----------- ------------ ----------- -----------
      Value          37.32        3.33         7.30       0.373       0.000
      Status        Normal HighWarning       Normal      Normal    LowAlarm
      HighAlarm      95.00        3.90        17.00       0.637       1.264
      HighWarning    90.00        3.70        14.00       0.637       0.791
      LowWarning    -20.00        2.90         2.00       0.082       0.028
      LowAlarm      -25.00        2.70         1.00       0.073       0.019
```

6.2 Modifying Port Operating Characteristics

You can make permanent or temporary changes to port operating characteristics. You make permanent port configuration changes using the Set Config Port command. These changes are saved in the active configuration and are preserved across switch or port resets. The Set Port command makes temporary changes that apply until the next port or switch reset, or until you activate a configuration.

The following example permanently changes the port 1 administrative state:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config port 1
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)   [Online] offline
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, A=Auto)            [Auto  ]
  PortType         (GL / G / F / FL / Donor)                      [GL    ]
  SymPortName      (string, max=32 chars)                         [Port1 ]
  ALFairness       (True / False)                                 [False ]
  DeviceScanEnable (True / False)                                 [True  ]
  ForceOfflineRSCN (True / False)                                 [False ]
  ARB_FF           (True / False)                                 [False ]
  InteropCredit    (decimal value, 0-255)                         [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)   [0     ]
  FANEnable        (True / False)                                 [True  ]
  AutoPerfTuning   (True / False)                                 [False ]
  LCFEnable        (True / False)                                 [False ]
  MFSEnable        (True / False)                                 [False ]
  VIEnable         (True / False)                                 [False ]
  MSEnable         (True / False)                                 [True  ]
  NoClose          (True / False)                                 [False ]
  IOStreamGuard    (Enable / Disable / Auto)                      [Disable]
  PDISCPingEnable  (True / False)                                 [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
SANbox (admin-config) #> config save
SANbox (admin-config) #> config activate
```

You can configure all ports based a specified source port using the Set Config Ports command. The following example configures ports 0–20 based on port 3.

```
SANbox #> admin start
SANbox (admin) config edit
SANbox (admin) #> set config ports 3
.
.
.
SANbox (admin-config)#> config save
SANbox (admin)#> config activate
SANbox (admin)#> admin end
```

The following example temporarily changes the port 1 administrative state to Down:

```
SANbox #> admin start
SANbox (admin) #> set port 1 state down
```

6.3 Port Binding

Port binding establishes up to 32 switches or devices that are permitted to log in to a particular switch port. Switches or devices that are not among the 32 are refused access to the port. Enter the Show Config Security Portbinding command to display the port binding configuration for all ports as shown in the following example.

```
SANbox #> show config security portbinding

  Configuration Name: default
  -------------------

  Port    Binding Status   WWN
  ----    --------------   -----------------------
  0       Enabled          10:20:30:40:50:60:70:80
  1       Enabled          10:20:30:40:50:60:70:80
  2       Disabled         10:20:30:40:50:60:70:80
  3       Enabled          10:20:30:40:50:60:70:80
  4       Enabled          10:20:30:40:50:60:70:80
  5       Disabled         10:20:30:40:50:60:70:80
  6       Enabled          10:20:30:40:50:60:70:81
  7       Disabled         10:20:30:40:50:60:70:82
  8       Enabled          10:20:30:40:50:60:70:80
```

Enter the Set Config Security Portbinding command to enable port binding for the selected port and to specify the world wide names of the authorized ports/devices. The following example enables port binding on port 1 and specifies two device world wide names.

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config security port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PortBindingEnabled (True / False)[False] true
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f9
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f8
  WWN                (N=None / WWN)[None ] n

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

6.4 Resetting a Port

Enter the Reset Port command to reinitialize one or more ports and to discard any temporary changes that have been made to the administrative state or link speed. The following example reinitializes port 1:

```
SANbox #> reset port 1
```

6.5 Configuring Port Threshold Alarms

The switch can monitor a set of port errors and generates alarms based on user-defined sample windows and thresholds. These port errors include the following:

- Cyclic Redundancy Check (CRC) errors
- Decode errors
- ISL connection count
- Device login errors
- Device logout errors
- Loss-of-signal errors

You make changes to the port threshold alarms by modifying the switch configuration as described in “Modify a Switch Configuration” on page 5-12. Refer to Table 13-18 for a description of the port alarm threshold parameters.

The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Enter the Set Config Threshold command to enable and configure port threshold monitoring on the switch:

```
SANbox #> admin start
SANbox  (admin) #> config edit
SANbox (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled     (True / False)              [False     ]
CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
ISLMonitoringEnabled           (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [2         ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LoginMonitoringEnabled         (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LogoutMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
 LOSMonitoringEnabled           (True / False)             [True      ]
  RisingTrigger                (decimal value, 1-1000)     [100       ]
  FallingTrigger               (decimal value, 0-1000)     [5         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

Finished configuring attributes.
This configuration must be saved (see config save command) and activated (see
config activate command) before it can take effect.
To discard this configuration use the config cancel command.
SANbox (admin-config) #> config save
SANbox (admin-config) #> config activate
```

6.6 Testing a Port

You can test a port using the Test Port command using online or offline tests. The following sections describe the test types, displaying test results, and cancelling a test:

- Online Tests for Ports
- Offline Tests for Ports
- Display Port Test Results
- Cancel a Port Test

6.6.1 Online Tests for Ports

An online test is a non-disruptive test that exercises the port, transceiver, and device connections. The port must be online and connected to a device. The following is an example of an online test:

```
SANbox #> admin start
SANbox (admin) #> test port 1 online

A list of attributes with formatting and current values will follow. Enter a new
value or simply press the ENTER key to accept the default value. If you wish to
terminate this process before reaching the end of the list press 'q' or 'Q' and the
ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [429496729]
FrameSize     (decimal value, 40-2148)        [256      ]
DataPattern   (32-bit hex value or 'Default') [Default  ]
StopOnError   (True / False)                  [True     ]
LoopForever   (True / False)                  [False    ]

Do you want to start the test? (y/n) [n] y

The test has been started.
A notification with the test result(s) will appear
on the screen when the test has completed.

SANbox (admin) #>
  Test for port 1 Passed.
```

6.6.2
Offline Tests for Ports

An offline test is a disruptive test that exercises the port connections. You must place the port in the diagnostics state using the Set Port command before starting the test. There are two types of offline test: internal loopback and external loopback.

- An internal loopback test exercises the internal port connections.
- An external loopback test exercises the port and its transceiver. A transceiver with a loopback plug is required for the port.

The following example performs an offline test:

```
SANbox #> admin start
SANbox (admin) #> set port 1 state diagnostics
SANbox (admin) #> test port 1 offline internal

  A list of attributes with formatting and current values will follow. Enter a new
  value or simply press the ENTER key to accept the default value. If you wish to
  terminate this process before reaching the end of the list press 'q' or 'Q' and
  the ENTER key to do so.

  LoopCount     (decimal value, 1-4294967295)   [429496729]
  FrameSize     (decimal value, 40-2148)        [256      ]
  DataPattern   (32-bit hex value or 'Default') [Default  ]
  StopOnError   (True / False)                  [True     ]
  LoopForever   (True / False)                  [False    ]

  Do you want to start the test? (y/n) [n] y

  The test has been started.
  A notification with the test result(s) will appear
  on the screen when the test has completed.

SANbox (admin) #>
  Test for port 1 Passed.
```

When the test is complete, remember to place the port back online.

```
SANbox (admin) #> set port 1 state online
```

6.6.3
Display Port Test Results

You can display the test status while the test is in progress by entering the Test Status Port command as shown in the following example:

```
SANbox (admin) #> test status port 1
Port              Test                Test               Loop      Test
Num      Port     Type                Status            Count  Failures
----     -------- ----                ------            -----  --------
1        1        Offline Internal    Passed               12         0
```

6.6.4
Cancel a Port Test

To cancel a port test that is in progress, enter the Test Cancel Port command.

6.7 Extending Port Transmission Distance

You can extend the distance over which an F_Port or G_Port port can transmit by borrowing buffer credits from other ports. Refer to the *SANbox 5000 Series Fibre Channel Switch Installation Guide* for information about extended credits and transmission distance. Enter the Set Config Port command to borrow and reallocate port credits as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config port
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the attributes
  for the port being processed, press 'q' or 'Q' and the ENTER key to do so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to so do.

  Configuring Port Number:  0
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, A=Auto)          [Auto  ]
  PortType         (GL / G / F / FL / Donor)                    [GL    ]  donor
  SymPortName      (string, max=32 chars)                       [Port0 ]  q

  Configuring Port Number:  1
  ------------------------
  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, A=Auto)          [Auto  ]
  PortType         (GL / G / F / FL / Donor)                    [G     ]
  SymPortName      (string, max=32 chars)                       [Port1 ]
  ALFairness       (True / False)                               [False ]
  DeviceScanEnable (True / False)                               [True  ]
  ForceOfflineRSCN (True / False)                               [False ]
  ARB_FF           (True / False)                               [False ]
  InteropCredit    (decimal value, 0-255)                       [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only) [0     ]  15
  FANEnable        (True / False)                               [True  ]  qq

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
SANbox (admin-config) #> config save
SANbox (admin-config) #> config activate
```

Enter the Show Donor command to display the extended credit status for the switch as shown in the following example:

```
SANbox #> show donor

  Port    Config Ext Credit Max Credit Donated Member of   Valid Groups to
  Number  Type   Requested  Available  to Port Donor Group Extend Credit
  ------  ------ ---------- ---------- ------- ----------- ---------------
  0       GL     0          16         None    0           0
  1       GL     0          16         None    0           0
  2       GL     0          16         None    0           0
  3       GL     0          16         None    0           0
  4       GL     0          16         None    0           0
  5       GL     0          16         None    0           0
  6       GL     0          16         None    0           0
  7       GL     0          16         None    0           0
  8       GL     0          16         None    0           0
  9       GL     0          16         None    0           0
  10      GL     0          16         None    0           0
  11      GL     0          16         None    0           0
  12      GL     0          16         None    0           0
  13      GL     0          16         None    0           0
  14      GL     0          16         None    0           0
  15      GL     0          16         None    0           0
  16      G      0          16         None    None        None
  Donor Group  Credit Pool
  -----------  -----------
  0            0
```

Section 7
Zoning Configuration

This section describes the following tasks:

- Displaying Zoning Database Information
- Configuring the Zoning Database
- Modifying the Zoning Database
- Resetting the Zoning Database
- Managing Zone Sets
- Managing Zones
- Managing Aliases

Consider device access needs within the fabric. Access is controlled by the use of zoning. Some zoning strategies include the following:

- Separate devices by operating system.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. A zone is a named group of ports or devices. Members of the same zone can communicate with each other and transmit outside the zone, but cannot receive inbound traffic from outside the zone. A port/device can be a member of up to eight zones whose combined membership does not exceed 64.

Zoning is hardware enforced on a switch port if the sum of the logged-in devices plus the devices zoned with devices on that port is 64 or less. If a port exceeds this sum, that port behaves as a soft zone member. The port continues to behave as a soft zone member until the sum of logged-in and zoned devices falls back to 64, and the port is reset.

A zone can be a component of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

7.1 Displaying Zoning Database Information

You can display the following information about the zoning database:

- Configured Zone Set Information
- Active Zone Set Information
- Zone Set Membership Information
- Zoning Modification History
- Zoning Database Limits

7.1.1 Configured Zone Set Information

The Zoneset List and the Zoning List commands display information about the all zone sets in the zoning database. Enter the Zoneset List command to display a list of the zone sets as shown in the following example:

```
SANbox #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

Enter the Zoning List command to display all zone sets, zones, and zone members in the zoning database as shown in the following example:

```
SANbox #> zoning list
  Active ZoneSet Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
  Configured Zoning Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:16
```

7.1.2
Active Zone Set Information

The Zoning Active and Zoneset Active commands display information about the active zone set. Enter the Zoning Active command to display component zones and zone members as shown in the following example:

```
SANbox #> zoning active
Active ZoneSet Information
  ZoneSet     Zone      ZoneMember
  -------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
```

Enter the Zoneset Active command to display the name of the active zone set and its activation history as shown in the following example:

```
SANbox #> zoneset active

  ActiveZoneSet    Bets
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

7.1.3
Zone Set Membership Information

The Zoneset Zones and Zone Zonesets commands display zone set membership information. Enter the Zoneset Zones command to display the member zones for a specified zone set as shown in the following example:

```
SANbox #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Enter the Zone Zonesets command to display the zone sets for which a specified zone is a member as shown in the following example:

```
SANbox #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  ---------------------------------
  zone_set_1
```

7.1.4
Zone Membership Information

Enter the Zone Members command to display the members for a specified zone as shown in the following example:

```
SANbox #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

7.1.5
Alias and Alias Membership Information

The Alias List and Alias Members commands display information about aliases. Enter the Alias List command to display a list of all aliases as shown in the following example:

```
SANbox #> alias list

  Current list of Zone Aliases
  ----------------------------
  alias1
  alias2
```

Enter the Alias Members command to display the membership for a specified alias as shown in the following example:

```
SANbox #> alias members alias1

  Current list of members for Zone Alias: alias1
  --------------------------------------
  50:06:04:82:bf:d2:18:c4
  50:06:04:82:bf:d2:18:c5
  50:06:04:82:bf:d2:18:c6
```

7.1.6
Zoning Modification History

Enter the Zoning History command to display a record of zoning modifications as shown in the following example:

```
SANbox #> zoning history
Active Database Information
  --------------------------
  ZoneSetLastActivated/DeactivatedBy  Remote
  ZoneSetLastActivated/DeactivatedOn  day mon date hh:mm:ss yyyy
  Database Checksum                   00000000

  Inactive Database Information
  ----------------------------
  ConfigurationLastEditedBy           admin@OB-session17
  ConfigurationLastEditedOn           day mon date hh:mm:ss yyyy
  Database Checksum                   00000000
```

History information includes the following:

- Time of the most recent zone set activation or deactivation and the user account that performed it
- Time of the most recent modifications to the zoning database and the user account that made them.
- Checksum for the zoning database

7.1.7
Zoning Database Limits

Enter the Zoning Limits command to display a summary of the objects in the zoning database and their maximum limit as shown in the following example:

```
SANbox #> zoning limits

  Zoning Attribute     Maximum   Current   [Zoning Name]
  ----------------     -------   -------   -------------
  MaxZoneSets          256       6
  MaxZones             2000      17
  MaxAliases           2500      1
  MaxTotalMembers      10000     166
  MaxZonesInZoneSets   2000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 24        Q_1Photon1
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 21        Q_2_NewJBOD2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

7.2 Configuring the Zoning Database

You can configure how the zoning database is applied to the switch and exchanged with the fabric through the zoning configuration parameters. The following zoning configuration parameters are available through the Set Config Zoning command. Refer to Table 13-19 for more information about the zoning configuration parameters.

- InteropAutoSave–This parameter enables or disables the saving of changes to active zone set in the switch's non-volatile memory.
- DefaultZone–This parameter enables or disables communication among ports/devices that are not defined in the active zone set.
- DiscardInactive–This parameter enables or disables the discarding of all zone sets except the active zone set.

If InteropAutoSave is False, you can revert zoning changes that have been received from another switch through the activation of a zone set, or merging of fabrics. Enter the Zoning Restore command to replace the volatile zoning database with the contents of the non-volatile zoning database.

To restore the zoning configuration to its factory values, enter the Reset Config or Reset Factory commands. Notice however, these commands restore other aspects of the switch configuration also.

To modify the zoning configuration, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through Telnet, Enterprise Fabric Suite 2007, or another management application. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name, the active configuration is assumed.

The Config Edit session provides access to the Set Config Zoning command as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> config edit
   The config named default is being edited.
SANbox (admin-config) #> set config zoning
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

  InteropAutoSave      (True / False)  [True ]
  DefaultZone          (True / False)  [True ]
  DiscardInactive      (True / False)  [False]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.

SANbox (admin-config)#> config save
SANbox (admin)#> config activate
SANbox (admin)#> admin end
```

7.3 Modifying the Zoning Database

To modify the zoning database, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time through Telnet, Enterprise Fabric Suite 2007, or another management application. You must also open a Zoning Edit session with the Zoning Edit command. The Zoning Edit session provides access to the Zoneset, Zone, Alias, and Zoning commands with which you make modifications to the zoning database.

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning)#> zoneset . . .
SANbox (admin-zoning)#> zone . . .
SANbox (admin-zoning)#> alias . . .
SANbox (admin-zoning)#> zoning . . .
```

When you are finished making changes, enter the Zoning Save command to save the changes and close the Zoning Edit session.

```
SANbox (admin-zoning)#> zoning save
```

To close the Zoning Edit session without saving changes, enter the Zoning Cancel command.

```
SANbox (admin-zoning)#> zoning cancel
```

Changes to the active zone set do not take effect until you activate it with the Zoneset Activate command. The active zone set is propagated throughout the fabric.

```
SANbox (admin)#> zoneset activate zoneset_1
SANbox (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

To remove all zoning database objects (aliases, zones, and zone sets) and restore the zoning database to its factory state, enter the Reset Zoning command as shown in the following example:

```
SANbox (admin) #> reset zoning
```

7.4 Resetting the Zoning Database

There are two ways to remove all aliases, zones, and zone sets from the zoning database:

- Enter the Zoning Clear command as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoning clear
SANbox (admin-zoning) #> zoning save
```

- Enter the Reset Zoning command as shown in the following example. The security configuration values, AutoSave, DefaultZone, and DiscardInactive remain unchanged. This is the preferred method.

```
SANbox #> admin start
SANbox (admin) #> reset zoning
```

7.5 Removing Inactive Zone Sets, Zones, and Aliases

Enter the Zoning Delete Orphan command to delete all objects from the zoning database except those in the active zone set.

```
SANbox #> admin start
SANbox (admin) #> zoning delete orphans
   This command will remove all zonesets, zones, and aliases
   that are not currently active.
Please confirm (y/n): [n] y
SANbox (admin) #> zoning save
```

7.6 Managing Zone Sets

Managing Zone Sets consists of the following tasks:

- Create a Zone Set
- Delete a Zone Set
- Rename a Zone Set
- Copy a Zone Set
- Add Zones to a Zone Set
- Remove Zones from a Zone Set
- Activate a Zone Set
- Deactivate a Zone Set

All of these tasks except Activate a Zone Set and Deactivate a Zone Set require an Admin session and a Zoning Edit session.

7.6.1 Create a Zone Set

Enter the Zoneset Create command to create a new zone set as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoneset create zoneset_1
SANbox (admin-zoning) #>zoning save
```

7.6.2 Delete a Zone Set

Enter the Zoneset Delete command to delete a zone set as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoneset delete zoneset_1
SANbox (admin-zoning) #>zoning save
```

7.6.3
Rename a Zone Set

Enter the Zoneset Rename command to rename a zone set as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoneset rename zoneset_old zoneset_new
SANbox (admin-zoning) #>zoning save
```

7.6.4
Copy a Zone Set

Enter the Zoneset Copy command to copy a zone set and its contents to a new zone set as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoneset copy zoneset_1 zoneset_2
SANbox (admin-zoning) #>zoning save
```

7.6.5
Add Zones to a Zone Set

Enter the Zoneset Add command to add a zone to a zone set as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoneset add zoneset_1 zone_1 zone_2
```

7.6.6
Remove Zones from a Zone Set

Enter the Zoneset Remove command to remove zones from a zone set as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zoneset remove zoneset_1 zone_1 zone_2
SANbox (admin-zoning) #>zoning save
```

7.6.7
Activate a Zone Set

Enter the Zoneset Activate command to apply zoning to the fabric as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoneset activate zoneset_1
```

7.6.8
Deactivate a Zone Set

Enter the Zoneset Deactivate command to deactivate the active zone set and disable zoning in the fabric:

```
SANbox #> admin start
SANbox (admin) #> zoneset deactivate
```

7.7
Managing Zones

Managing Zones consists of the following tasks:

- Create a Zone
- Delete a Zone
- Rename a Zone
- Copy a Zone
- Add Members to a Zone
- Remove Members from a Zone

All of these tasks require an Admin session and a Zoning Edit session.

7.7.1
Create a Zone

Enter the Zone Create command to create a new zone as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zone create zone_1
SANbox (admin-zoning) #> zoning save
```

7.7.2
Delete a Zone

Enter the Zone Delete command to delete zone_1 from the zoning database as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zone delete zone_1
SANbox (admin-zoning) #> zoning save
```

7.7.3 Rename a Zone

Enter the Zone Rename command to rename zone_1 to zone_a as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zone rename zone_1 zone_a
SANbox (admin-zoning) #> zoning save
```

7.7.4 Copy a Zone

Enter the Zone Copy command to copy the contents of an existing zone (zone_1) to a new zone (zone_2) as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zone copy zone_1 zone_2
SANbox (admin-zoning) #> zoning save
```

7.7.5 Add Members to a Zone

Enter the Zone Add command to add ports/devices to zone_1 as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zone add zone_1 alias_1 1,4 1,5
SANbox (admin-zoning) #> zoning save
```

7.7.6 Remove Members from a Zone

Enter the Zone Remove command to remove ports/devices from zone_1 as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> zone remove zone_1 alias_1 1,4 1,5
SANbox (admin-zoning) #> zoning save
```

7.8 Managing Aliases

Managing aliases consists of the following tasks:

- Create an Alias
- Delete an Alias
- Rename an Alias
- Copy an Alias
- Add Members to an Alias
- Remove Members from an Alias

All of these tasks require an Admin session and a Zoning Edit session.

7.8.1 Create an Alias

Enter the Alias Create command to create a new alias as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> alias create alias_1
SANbox (admin-zoning) #> zoning save
```

7.8.2 Delete an Alias

Enter the Alias Delete command to delete alias_1 from the zoning database as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> alias delete alias_1
SANbox (admin-zoning) #> zoning save
```

7.8.3 Rename an Alias

Enter the Alias Rename command to rename alias_1 to alias_a as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> alias rename alias_1 alias_a
SANbox (admin-zoning) #> zoning save
```

7.8.4
Copy an Alias

Enter the Alias Copy command to copy alias_1 and its contents to alias_2 as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> alias copy alias_1 alias_2
SANbox (admin-zoning) #> zoning save
```

7.8.5
Add Members to an Alias

Enter the Alias Add command to add ports/devices to alias_1 as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> alias add alias_1  1,4 1,5
SANbox (admin-zoning) #> zoning save
```

7.8.6
Remove Members from an Alias

Enter the Alias Remove command to remove ports/devices from alias_1 as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #> alias remove alias_1 1,4 1,5
SANbox (admin-zoning) #> zoning save
```

Section 8

Connection Security Configuration

NOTE: SSH and SSL connection security require the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller.

This section describes the following tasks:

- Managing SSL and SSH Services
- Displaying SSL and SSH Services
- Creating an SSL Security Certificate

The switch supports secure connections with Telnet and switch management applications. The Secure SHell protocol (SSH) secures Telnet connections to the switch. The Secure Sockets Layer (SSL) protocol secures switch connections to the following management applications:

- Enterprise Fabric Suite 2007
- QuickTools
- Application Programming Interface
- Storage Management Initiative-Specification (SMI-S)

8.1 Managing SSL and SSH Services

Consider the following when enabling SSH and SSL services:

- To establish a secure Telnet connection, your workstation must use an SSH client.
- To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. Refer to “Setting the Date and Time” on page 5-17.
- The SSL service must be enabled to authenticate users through a RADIUS server. Refer to “Configuring a RADIUS Server on the Switch” on page 10-3.
- To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.
- Enabling SSL automatically creates a security certificate on the switch.

Enter the Set Setup Services command to manage both SSH and SSL services as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> set setup services
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False] True
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False] True
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]

  Do you want to save and activate this services setup? (y/n): [n] y
```

8.2 Displaying SSL and SSH Services

Enter the Show Setup Services command to display the status of the SSH and SSL services as shown in the following example:

```
SANbox #> show setup services
System Services
----------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLEnabled                False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
MgmtServerEnabled         True
```

8.3 Creating an SSL Security Certificate

Enabling SSL automatically creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as Enterprise Fabric Suite 2007. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the original certificate become invalid, enter the Create Certificate command to create a new one as shown in the following example:

```
SANbox (admin) #> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

To ensure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. Refer to “Setting the Date and Time” on page 5-17.

Notes

Section 9

Device Security Configuration

NOTE: Device security requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller.

This section describes the following tasks:

- Displaying Security Database Information
- Configuring the Security Database
- Modifying the Security Database
- Resetting the Security Database
- Managing Security Sets
- Managing Groups

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands.

Device security is defined through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security database is made up of all security sets on the switch.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using a Remote Dial-In User Service (RADIUS) server such as Microsoft® RADIUS.

9.1 Displaying Security Database Information

You can display the following information about the security database:

- Configured Security Set Information
- Active Security Set Information
- Security Set Membership Information
- Group Membership Information
- Security Database Modification History
- Security Database Limits

9.1.1 Configured Security Set Information

The Securityset List and the Security List commands display information about the all security sets in the security database. Enter the Securityset List command to display a list of the security sets as shown in the following example:

```
SANbox #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

Enter the Security List command to display all security sets, groups, and group members in the security database as shown in the following example:

```
SANbox #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

9.1.2
Active Security Set Information

The Security Active and Securityset Active commands display information about the active security set. Enter the Security Active command to display component groups and group members as shown in the following example:

```
SANbox #> security active
  Active Security Information

  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

Enter the Securityset Active command to display the name of the active security set and its activation history as shown in the following example:

```
SANbox #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet alpha
  LastActivatedBy  Remote
  LastActivatedOn  day month date time year
```

9.1.3
Security Set Membership Information

The Securityset Groups and Group Securitysets commands display security set membership information. Enter the Securityset Groups command to display the member groups for a specified security set as shown in the following example:

```
SANbox #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  ---------------------------------------
  group1 (ISL)
  group2 (Port)
```

Enter the Group Securitysets command to display the security sets for which a specified group is a member as shown in the following example:

```
SANbox #> group securitysets group_1

  Current list of SecuritySets for Group: group_1
  ---------------------------------------
  SecuritySet_1
  SecuritySet_2
  SecuritySet_A
  SecuritySet_B
```

9.1.4
Group Membership Information

Enter the Group Members command to display the members for a specified group as shown in the following example:

```
SANbox #> group members group_1
  Current list of members for Group: group_1
  ---------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

9.1.5
Security Database Modification History

Enter the Security History command to display a record of security database modifications as shown in the following example:

```
SANbox #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  day month date time year
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           day month date time year
  Database Checksum                   00007558
```

History information includes the following:

- Time of the most recent security set activation or deactivation and the user account that performed it
- Time of the most recent modifications to the security database and the user account that made them
- Checksum for the security database

9.1.6
Security Database Limits

Enter the Security Limits command to display a summary of the objects in the security database and their maximum limit as shown in the following example:

```
SANbox #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

9.2 Configuring the Security Database

You can configure how the security database is applied to the switch and exchanged with the fabric through the security configuration parameters. The following security configuration parameters are available through the Set Config Security command:

- AutoSave–This parameter enables or disables the saving of changes to active security set in the switch's non-volatile security database.
- FabricBindingEnabled–This parameter enables or disables the configuration and enforcement of fabric binding on all switches in the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

If AutoSave is False, you can revert device security changes that have been received from another switch through the activation of a security set, or merging of fabrics. Enter the Security Restore command to replace the volatile security database with the contents of the non-volatile security database.

To restore the security configuration to its factory values, you can enter the Reset Config or Reset Factory command. Notice however, that these commands restore other aspects of the switch configuration also.

To modify the security configuration, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or Enterprise Fabric Suite 2007. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name, the active configuration is assumed. The Config Edit session provides access to the Set Config Security command as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config security
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  FabricBindingEnabled  (True / False)     [False]
  AutoSave              (True / False)     [True ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.

SANbox (admin-config)#> config save
SANbox (admin)#> config activate
SANbox (admin)#> admin end
```

9.3 Modifying the Security Database

To modify the security database, you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or Enterprise Fabric Suite 2007. You must also open a Security Edit session with the Security Edit command. The Security Edit session provides access to the Securityset, Group, and Security commands with which you make modifications to the security database.

```
SANbox #> admin start
SANbox (admin) #> security edit
SANbox (admin-security)#> securityset . . .
SANbox (admin-security)#> group . . .
SANbox (admin-security)#> security . . .
```

When you are finished making changes, enter the Security Save command to save the changes and close the Security Edit session.

```
SANbox (admin-security)#> security save
```

To close the session without saving changes, enter the Security Cancel command.

```
SANbox (admin-security)#> security cancel
```

Changes to the active security set do not take effect until you activate it with the Security Activate command. The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

```
SANbox (admin)#> security activate
SANbox (admin)#> admin end
```

9.4 Resetting the Security Database

There are two ways to remove all groups and security sets from the security database:

- Enter the Security Clear command as shown in the following example:

```
SANbox (admin-security) #> security clear
  All security information will be cleared.  Please confirm (y/n): [n] y
SANbox (admin-security) #> security save
```

- Enter the Reset Security command as shown in the following example. The security configuration values, autosave and fabric binding remain unchanged.

```
SANbox (admin) #> reset security
```

9.5 Managing Security Sets

Managing Security Sets consists of the following tasks:

- Create a Security Set
- Delete a Security Set
- Rename a Security Set
- Copy a Security Set
- Add Groups to a Security Set
- Remove Groups from a Security Set
- Activate a Security Set
- Deactivate a Security Set

All of these tasks except Activate a Security Set and Deactivate a Security Set require a Security Edit session.

9.5.1 Create a Security Set

Enter the Securityset Create command to create a new security set as shown in the following example:

```
SANbox (admin-security) #> securityset create securityset_1
```

9.5.2 Delete a Security Set

Enter the Securityset Delete command to delete a security set as shown in the following example:

```
SANbox (admin-security) #> securityset delete securityset_1
```

9.5.3 Rename a Security Set

Enter the Securityset Rename command to rename a security set as shown in the following example:

```
SANbox (admin-security) #> securityset rename securityset_old securityset_new
```

9.5.4 Copy a Security Set

Enter the Securityset Copy command to copy a security set and its contents to a new security set as shown in the following example:

```
SANbox (admin-security) #> securityset copy securityset_1 securityset_2
```

9.5.5
Add Groups to a Security Set

Enter the Securityset Add command to add a group to a security set as shown in the following example:

```
SANbox (admin-security) #> securityset add securityset_1 group_isl group_port
```

9.5.6
Remove Groups from a Security Set

Enter the Securityset Remove command to remove groups from a security set as shown in the following example:

```
SANbox (admin-security) #> sescurityset remove securityset_1 group_isl group_port
```

9.5.7
Activate a Security Set

Enter the Securityset Activate command to apply security to the fabric as shown in the following example:

```
SANbox (admin) #> securityset activate securityset_1
```

9.5.8
Deactivate a Security Set

Enter the Securityset Deactivate command to deactivate the active security set and disable security in the fabric:

```
SANbox (admin) #> securityset deactivate
```

9.6 Managing Groups

Managing Groups consists of the following tasks:

- Create a Group
- Delete a Group
- Rename a Group
- Copy a Group
- Add Members to a Group
- Modify a Group Member
- Remove Members from a Group

All of these tasks require an Admin session and a Security Edit session.

9.6.1 Create a Group

Creating a group involves specifying a group name and a group type. There are three types of groups:

- ISL group–secures connected switches
- Port group–secures connected devices
- MS group–secures management server commands

Enter the Group Create command to create a new port group as shown in the following example:

```
SANbox (admin-security) #> group create group_port port
```

9.6.2 Delete a Group

Enter the Group Delete command to delete group_port from the security database as shown in the following example:

```
SANbox (admin-security) #> group delete group_port
```

9.6.3 Rename a Group

Enter the Group Rename command to rename group_port to port_1 as shown in the following example:

```
SANbox (admin-security) #> group rename group_port port_1
```

9.6.4
Copy a Group

Enter the Group Copy command to copy the contents of an existing group (group_port) to a new group (port_1) as shown in the following example:

```
SANbox (admin-security) #> group copy group_port port_1
```

9.6.5
Add Members to a Group

Adding a member to a group involves specifying a group, the member worldwide name, and the member attributes. The member attributes define the authentication method, encryption method, secrets, and fabric binding, depending on the group type.

- For ISL member attributes, refer to Table 13-1.
- For Port member attributes, refer to Table 13-2.
- For MS member attributes, refer to Table 13-3.

Enter the Group Add command to add a member to a group:

```
SANbox (admin-security) #> group add group_1
  A list of attributes with formatting and default values will follow
  Enter a new value or simply press the ENTER key to accept the current value
  with exception of the Group Member WWN field which is mandatory.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name       group_1
  Group Type       ISL
  Member          (WWN)                        [00:00:00:00:00:00:00:00] 10:00:00:c0:dd:00:90:a3
  Authentication  (None / Chap)                    [None                   ]chap
  PrimaryHash     (MD5 / SHA-1)                    [MD5                    ]
  PrimarySecret   (32 hex or 16 ASCII char value)  [                       ]0123456789abcdef
  SecondaryHash   (MD5 / SHA-1 / None)             [None                   ]
  SecondarySecret (40 hex or 20 ASCII char value)  [                       ]
  Binding         (domain ID 1-239, 0=None)        [0                      ]

  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

9.6.6
Modify a Group Member

Modifying a group member involves changing the member attributes. The member attributes define the authentication method, encryption methods, secrets, and fabric binding, depending on the group type.

- For ISL member attributes, refer to Table 13-1.
- For Port member attributes, refer to Table 13-2.
- For MS member attributes, refer to Table 13-3.

Enter the Group Edit command to change the attributes of a group member:

```
SANbox #> admin start
SANbox (admin) #> security edit
SANbox (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name        g1
  Group Type        ISL
  Group Member      10:00:00:c0:dd:00:90:a3
  Authentication    (None / Chap)                   [None]  chap
  PrimaryHash       (MD5 / SHA-1)                   [MD5 ]  sha-1
  PrimarySecret     (40 hex or 20 ASCII char value) [    ]  12345678901234567890
  SecondaryHash     (MD5 / SHA-1 / None)            [None]  md5
  SecondarySecret   (32 hex or 16 ASCII char value) [    ]  1234567890123456
  Binding           (domain ID 1-239, 0=None)       [3   ]

  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

9.6.7
Remove Members from a Group

Enter the Group Remove command to remove a member from a group as shown in the following example:

```
SANbox (admin-security) #> group remove group_1 10:00:00:c0:dd:00:90:a3
```

Section 10

RADIUS Server Configuration

NOTE: RADIUS server configuration requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller.

Authentication can be performed locally using the switch's security database, or remotely using a Remote Dial-In User Service (RADIUS) server such as Microsoft RADIUS. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts. Refer to Section 3 for information about user accounts. A secure connection is required to authenticate user logins with a RADIUS server. Refer to Section 8 for information about secure connections.

This section describes the following tasks:

- Displaying RADIUS Server Information
- Configuring a RADIUS Server on the Switch

10.1 Displaying RADIUS Server Information

Enter the Show Setup Radius command to display RADIUS server information as shown in the following example. Refer to Table 13-20 for a description of the RADIUS server configuration parameters.

```
SANbox #> show setup radius

  Radius Information
  ------------------
  DeviceAuthOrder   RadiusLocal
  UserAuthOrder     RadiusLocal
  TotalServers      1

  Server: 1

  ServerIPAddress   10.20.11.8
  ServerUDPPort     1812
  DeviceAuthServer  False
  UserAuthServer    True
  AccountingServer  False
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********
```

10.2 Configuring a RADIUS Server on the Switch

Enter the Set Setup Radius command to configure a RADIUS server on the switch as shown in the following example. Refer to Table 13-20 for a description of the RADIUS server configuration parameters.

```
SANbox (admin) #> set setup radius

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the attributes
  for the server being processed, press 'q' or 'Q' and the ENTER key to do so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to so do.

  DeviceAuthOrder   (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  UserAuthOrder     (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  TotalServers      (decimal value, 0-5)               [1    ]

  Server: 1
  ServerIPAddress   (dot-notated IP Address)         [10.20.11.8]
  ServerUDPPort     (decimal value)                  [1812      ]
  DeviceAuthServer  (True / False)                   [True      ]
  UserAuthServer    (True / False)                   [True      ]
  AccountingServer  (True / False)                   [False     ]
  Timeout           (decimal value, 10-30 secs)      [10        ]
  Retries           (decimal value, 1-3, 0=None)     [0         ]
  SignPackets       (True / False)                   [False     ]
  Secret            (1-63 characters, recommend 22+) [**********]
  Do you want to save and activate this radius setup? (y/n): [n]
```

Notes

Section 11

Event Log Configuration

This section describes the following tasks:

- Starting and Stopping Event Logging
- Displaying the Event Log
- Managing the Event Log Configuration
- Clearing the Event Log
- Logging to a Remote Host
- Creating and Downloading a Log File

Event messages originate from the switch or from the management application in response to events that occur in the fabric. Refer to the *SANbox Fibre Channel Switch Event Message Guide* for a complete listing of switch event messages.

Events are classified by the following severity levels:

- Alarm–The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen. Alarm thresholds can be defined for certain port errors to customize when to generate an alarm.
- Critical–The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.
- Warning–The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.
- Informative–The informative level describes routine events associated with a normal fabric.

11.1 Starting and Stopping Event Logging

Enter the Set Log Stop command to stop recording event messages in the switch Log as shown in the following example:

```
SANbox (admin) #> set log stop
```

Enter the Set Log Start command to start recording event message in the switch log as shown in the following example:

```
SANbox (admin) #> set log start
```

11.2 Displaying the Event Log

Enter the Show Log command to display the event log. Each message has the following format:

[ordinal][time_stamp][severity][message_ID][source][message_text]

`[ordinal]`–A number assigned to each message in sequence since the last time the alarm history was cleared.

`[time_stamp]`–The time the alarm was issued in the format day month hh:mm:ss.ms UTC yyyy. This time stamp comes from the switch for events that originate with the switch, and from the workstation for events that originate with Enterprise Fabric Suite 2007.

`[severity]`–The event severity: A–Alarm, C–Critical, W–Warning, I–Informative.

`[message_ID]`–A number that identifies the message using the following format: category.message_number

`[source]`–The program module or application that generated the event. Sources include Zoning, Switch, PortApp, EPort, Management Server. Alarms do not include the source.

`[message_text]`–The message text

The following is an example of the Show Log command:

```
SANbox #> show log
   [327][day month date time year][I][Eport Port:0/8][Eport State=
   E_A0_GET_DOMAIN_ID]
   [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
   [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
   [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
   [331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
   [332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
   len= 0x30]
   [333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
   [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
   [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
```

You can also filter the event log display with the Show Log Display command and customize the messages that display automatically in the output stream.

- Filtering the Event Log Display
- Controlling Messages in the Output Stream

11.2.1
Filtering the Event Log Display

You can customize what events are displayed according to the component or severity level. Enter the Show Log Display command to filter the events in the display. You can choose from the following severity levels and component events:

- Informative events
- Warning events
- Critical events
- E_Port events
- Management server events
- Name server events
- Port events
- Switch management events
- Simple Network Management Protocol (SNMP) events
- Zoning events

The following example filters the event log display for critical events.

```
SANbox #> show log display critical
```

11.2.2
Controlling Messages in the Output Stream

Enter the Set Log Display command to specify the severity level filter to use to determine what messages are automatically displayed on the screen when they occur. Alarms are always included in the output stream. The following example includes warning and critical level messages in the output stream:

```
SANbox (admin) #> set log display warn
```

11.3 Managing the Event Log Configuration

Managing the Event Log Configuration consists of the following tasks:

- Configure the Event Log
- Display the Event Log Configuration
- Restore the Event Log Configuration

11.3.1 Configure the Event Log

You can customize what events are recorded in the switch event log according to component, severity level, and port. Enter the Set Log Component, Set Log Level, and Set Log Port commands to filter the events to be recorded. You can choose from the following component events:

- E_Port events
- Management server events
- Name server events
- Port events
- Switch management events
- Simple Network Management Protocol (SNMP) events
- Zoning events

The following example configures the event log to record switch management events with warning and critical severity levels associated with ports 0–3. Entering the Set Log Save command ensures that this configuration is preserved across switch resets.

```
SANbox (admin) #> set log component switch
SANbox (admin) #> set log level warn
SANbox (admin) #> set log port 0 1 2 3
SANbox (admin) #> set log save
```

11.3.2
Display the Event Log Configuration

Enter the Show Log Settings command to display all event log configuration settings as shown in the following example:

```
SANbox #> show log settings
Current settings for log
------------------------
Started             True
FilterComponent     NameServer MgmtServer Zoning Switch Blade Port Eport Snmp CLI
FilterLevel         Info
DisplayLevel        Critical
FilterPort          0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
```

11.3.3
Restore the Event Log Configuration

Enter the Set Log Restore command to return the event log configuration to the factory default as shown in the following example:

```
SANbox (admin) #> set log restore
```

11.4
Clearing the Event Log

Enter the Set Log Clear command to delete all entries in the event log as shown in the following example:

```
SANbox (admin) #> set log clear
```

11.5 Logging to a Remote Host

The switch comes from the factory with local logging enabled, which instructs the switch firmware to maintain an event log in switch memory. The switch can also be configured to log events to a remote host that supports the syslog protocol. This requires that you enable remote logging on the switch and specify an IP address for the remote host.

NOTE: To log event messages on a remote host, you must edit the syslog.conf file on the remote host and then restart the syslog daemon. The syslog.conf file must contain an entry that specifies the name of the log file. Add the following line to the syslog.conf file. A <tab> separates the selector field (local0.info) and action field which contains the log file path name (/var/adm/messages/messages.name).

```
local0.info <tab> /var/adm/messages/messages.name
```

Consult your host operating system documentation for information on how to configure remote logging.

The Set Setup System command controls local logging through the LocalLogEnabled parameter and remote logging through the RemoteLogEnabled and RemoteLogHostAddress parameters as shown in the following example:

```
SANbox (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

EthNetworkDiscovery     (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
EthNetworkAddress       (dot-notated IP Address)             [10.0.0.1     ]
EthNetworkMask          (dot-notated IP Address)             [255.255.255.0]
EthGatewayAddress       (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
InactivityTimeout       (dec value 0-1440 minutes, 0=never)  [0            ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
NTPClientEnabled        (True / False)                       [False        ]
NTPServerAddress        (dot-notated IP Address)             [10.0.0.254   ]
EmbeddedGUIEnabled      (True / False)                       [True         ]
```

11.6 Creating and Downloading a Log File

Enter the Set Log Archive command to collect the event log messages in a file on the switch named *logfile*. This file can have a maximum of 1200 event messages. Use FTP to download the file from the switch to your workstation as follows:

1. Log into the switch through Telnet and create an archive of the event log. The Set Log Archive command creates a file on the switch named *logfile*.

```
SANbox  #> admin start
SANbox (admin) #> set log archive
```

2. Open an FTP session on the switch and log in with the account name *images* and password *images*. Transfer the file *logfile* in binary mode with the Get command.

```
>ftp ip_address
user:images
password: images

ftp>bin
ftp>get logfile
    xxxxx bytes sent in xx secs.
ftp>quit
```

Notes

Section 12

Simple Network Management Protocol Configuration

This section describes the following tasks:

- Managing the SNMP Service
- Displaying SNMP Information
- Modifying the SNMP Configuration
- Resetting the SNMP Configuration

The Simple Network Management Protocol (SNMP) provides for the management of the switch through third-party applications that use SNMP. Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to well-known defaults and should be changed if SNMP is to be enabled.

12.1 Managing the SNMP Service

You control the SNMP service SNMPEnabled parameters through the Set Setup SNMP or Set Setup Services commands. Refer to “Modifying the SNMP Configuration” on page 12-4 for more information.

Enter the Set Setup Services command to enable SNMP as shown in the following example:

```
SANbox #> admin start
SANbox (admin) #> set setup services

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False]
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False]
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]

  Do you want to save and activate this services setup? (y/n): [n]
```

You can display the SNMPEnabled parameters using the Show Setup SNMP or Show Setup Services commands.

12.2 Displaying SNMP Information

Enter the Show Setup SNMP command to display SNMP configuration information as shown in the following example. Refer to Table 13-22 for a description of the SNMP parameters.

```
SANbox #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           SANbox 5000 FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
  ObjectID              1.3.6.1.4.1.1663.1.1.1.1.17
  AuthFailureTrap       True
  ProxyEnabled          True
```

12.3 Modifying the SNMP Configuration

Enter the Set Setup SNMP command to modify the SNMP configuration as shown in the following example. Refer to Table 13-22 for SNMP parameters descriptions.

```
SANbox (admin) #> set setup snmp

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Trap Severity Options

  --------------------

  unknown, emergency, alert, critical, error, warning, notify, info, debug, mark
  SNMPEnabled         (True / False)               [True             ]
  Contact             (string, max=64 chars)      [<sysContact undefined>]
  Location            (string, max=64 chars)      [<sysLocation undefined>]
  Trap1Address        (dot-notated IP Address)    [10.20.71.15      ]
  Trap1Port           (decimal value)             [162              ]
  Trap1Severity       (see allowed options above) [warning          ]
  Trap1Version        (1 / 2)                     [2                ]
  Trap1Enabled        (True / False)              [False            ]
  Trap2Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap2Port           (decimal value)             [162              ]
  Trap2Severity       (see allowed options above) [warning          ]
  Trap2Version        (1 / 2)                     [2                ]
  Trap2Enabled        (True / False)              [False            ]
  Trap3Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap3Port           (decimal value)             [162              ]
  Trap3Severity       (see allowed options above) [warning          ]
  Trap3Version        (1 / 2)                     [2                ]
  Trap3Enabled        (True / False)              [False            ]
  Trap4Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap4Port           (decimal value)             [162              ]
  Trap4Severity       (see allowed options above) [warning          ]
  Trap4Version        (1 / 2)                     [2                ]
  Trap4Enabled        (True / False)              [False            ]
  Trap5Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap5Port           (decimal value)             [162              ]
  Trap5Severity       (see allowed options above) [warning          ]
  Trap5Version        (1 / 2)                     [2                ]
  Trap5Enabled        (True / False)              [False            ]
  ReadCommunity       (string, max=32 chars)      [public           ]
  WriteCommunity      (string, max=32 chars)      [private          ]
  TrapCommunity       (string, max=32 chars)      [public           ]
  AuthFailureTrap     (True / False)              [False            ]
  ProxyEnabled        (True / False)              [True             ]
```

12.4 Resetting the SNMP Configuration

Enter the Reset SNMP command to reset the SNMP configuration back to the factory defaults as shown in the following example. Refer to Table 13-9 for a listing of the SNMP configuration factory defaults.

```
SANbox (admin) #> reset snmp
```

Notes

Section 13

Command Reference

This section describes the commands of the CLI and the format in which they are presented. The command format presents the following:

- Access Authority
- Syntax and Keywords
- Notes and Examples

The commands are listed in “Command Listing” on page 13-3.

13.1 Access Authority

The **Authority** paragraph in each command description indicates what types of sessions are required to enter that command. Commands associated with monitoring tasks are available to all account names with no special session requirement. Commands associated with configuration tasks are available only within an Admin session. An account must have Admin authority to enter the Admin Start command, which opens an Admin session.

Some commands require that you open additional editing sessions within an Admin session such as the following:

- Commands that modify zoning require a Zoning Edit session, which is opened by the Zoning Edit command. These commands include the Alias, Zone, Zoneset, and Zoning commands.
- Commands that modify device security require a Security Edit session, which is opened by the Security Edit command. These command include the Group, Security, and Securityset commands.
- Commands that modify the switch configuration require a Config Edit session, which is opened by the Config Edit command. These command include all of the Set Config commands.

13.2 Syntax and Keywords

The **Syntax** paragraph defines the command syntax using the following convention:

command

keyword
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example, the **delete** keyword can be abbreviated **del**.

The **Keywords** paragraph lists and describes each keyword and any applicable values.

13.3 Notes and Examples

The **Notes** paragraph presents useful information about the command and its use, including special applications or effects on other commands. The **Examples** paragraph presents sample screen captures of the command and its output.

13.4 Command Listing

The commands are listed in alphabetical order as follows:

A Admin, Alias

C Config, Create

D Date

E Exit

F Fcping, Fctrace, Feature, Firmware Install

G Group

H Hardreset, Help, History, Hotreset

I Image

L Lip, Logout

P Passwd, Ping, Ps

Q Quit

R Reset

S Security, Securityset, Set Alarm, Set Beacon
Set Config Port through Set Config Zoning
Set Log, Set Pagebreak, Set Port
Set Setup Radius through Set Setup System
Set Switch State, Set Timezone

Sh Show About, Show Alarm, Show Broadcast, Show Chassis
Show Config Port through Show Config Zoning
Show Domains, Show Donor, Show Fabric, Show FDMI,
Show Interface, Show Log, Show LSDB, Show Media, Show Mem, Show NS,
Show Pagebreak, Show Perf, Show Port, Show Post Log
Show Setup Mfg through Show Setup System
Show Switch, Show Timezone, Show Topology, Show Users,
Show Version, Shutdown

T Test Cancel, Test Port, Test Status

U,W,Z Uptime, User, Whoami, Zone, Zoneset, Zoning

Admin

Opens and closes an Admin session. The Admin session provides access to commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command.

Authority User account with Admin authority

Syntax **admin**

start (or begin)
end (or stop)
cancel

Keywords **start (or begin)**

Opens the Admin session

end (or stop)

Closes the Admin session. The Hardreset, Hotreset, Quit, Shutdown, and Reset Switch commands will also end an Admin session.

cancel

Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an Admin session does not release the session. In this case, you must either wait for the Admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
SANbox #> admin start
SANbox (admin) #>
.
.
.
SANbox (admin) #> admin end
```

Alias

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session and Zoning Edit session for all keywords except List and Members

Syntax **alias**

add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Keywords **add [alias] [member_list]**

Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]

Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]

Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]

Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all aliases. This keyword does not require an Admin session.

members [alias]

Displays all members of the alias given by [alias]. This keyword does not require an Admin session.

remove [alias] [member_list]

Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]

Renames the alias given by [alias_old] to the alias given by [alias_new].

Examples

The following is an example of the Alias List command:

```
SANbox #> alias list

  Current list of Zone Aliases
  ----------------------------
  alias1
  alias2
```

The following is an example of the Alias Members command:

```
SANbox #> alias members alias1

  Current list of members for Zone Alias: alias1
  --------------------------------------
  50:06:04:82:bf:d2:18:c4
  50:06:04:82:bf:d2:18:c5
  50:06:04:82:bf:d2:18:c6
```

Config

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, refer to the "Set Config Switch" command on page 13-70.

Authority Admin session for all keywords except Backup and List

Syntax

config
activate *[config_name]*
backup
cancel
copy [config_source] [config_destination]
delete [config_name]
edit *[config_name]*
list
restore
save *[config_name]*

Keywords

activate *[config_name]*

Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

backup

Creates a file named *configdata*, which contains the system configuration information. This keyword does not require an Admin session. Configuration backup files are deleted from the switch during a power cycle or switch reset.

cancel

Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]

Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config_name]

Deletes the configuration given by [config_name] from the switch. You cannot delete the default configuration (Default Config) nor the active configuration.

edit *[config_name]*

Opens an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.

list

Displays a list of all available configurations on the switch. This keyword does not require an Admin session.

restore

Restores configuration settings to an out-of-band switch from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command. After the restore is complete, the switch automatically resets. Refer to "Back Up and Restore a Switch Configuration" on page 5-14.

NOTE:

- If the restore process changes the IP address, use the Set Setup System command to return the IP configuration to the values you want. If the IP address is unknown, you must place the switch in maintenance mode and reset the network configuration to restore the default IP address 10.0.0.1. Refer to the installation guide for information about using maintenance mode.
- Configuration archive files created with the Enterprise Fabric Suite 2007 Archive function are not compatible with the Config Restore command.
- The *configdata* backup file does not include the security group primary or secondary secrets, and therefore are not restored. You must edit the security database and reconfigure the secrets. If they are not, the switch will isolate from the fabric.

save *[config_name]*

Saves changes made during a configuration edit session in the configuration given by [config_name]. If you omit [config_name], the value for [config_name] you chose for the most recent Config Edit command is used. [config_name] can be up to 31 characters excluding #, semicolon (;), and comma (,). The switch supports up to 10 configurations including the default configuration.

Notes

Changes you make to an active or inactive configuration can be saved, but will not take effect until you activate that configuration.

Examples

The following shows an example of how to open and close a Config Edit session:

```
SANbox #> admin start
SANbox (admin) #> config edit
   The config named default is being edited.
.
.
SANbox (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
SANbox (admin) #> admin end
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

```
SANbox #> config backup
SANbox #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```

The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

SANbox #> admin start
SANbox (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is being
restored -  this could take several minutes]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be reset in
3 seconds due to a config restore]
SANbox (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being reset]
```

Create

Creates support files for troubleshooting switch problems, and certificates for secure communications for Enterprise Fabric Suite 2007 and SMI-S.

Authority Admin session for the Certificate keyword

Syntax **create**

certificate

support

Keywords **certificate**

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as Enterprise Fabric Suite 2007. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the current certificate become invalid, use the Create Certificate command to create a new one.

NOTE: To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. Refer to the following:

- "Date" command on page 13-13 for information about setting the time and date
- "Set Timezone" command on page 13-96 for information about setting the time zone on the switch and workstation
- "Set Setup System" command on page 13-93 (System keyword) for information about enabling the Network Time Protocol for synchronizing the time and date on the switch and workstation from an NTP server.

support

Assembles all log files and switch memory data into a file (dump_support.tgz) on the switch. If your workstation has an FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation. The support file is useful to technical support personnel for troubleshooting switch problems. Use this command when directed by your authorized maintenance provider. This keyword does not require an Admin session.

NOTE: Support files are deleted from the switch during a power cycle, switch reset, or a transfer of the primary role to the secondary CPU blade.

Examples

The following is an example of the Create Support command when an FTP server is available on the workstation:

```
SANbox #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): y
Enter IP Address of remote computer: 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
Would you like to continue downloading support file? (y/n) [n]: y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password:  xxxxxxx

230 User johndoe logged in.
cd bin/support
250 CWD command successful.
lcd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

The following is an example of the Create Support command and how to download the support file to your workstation. When prompted to send the support file to another machine, decline, then close the Telnet session. Open an FTP session on the switch and log in with the account name *images* and password *images*. Transfer the dump_support.tgz file in binary mode with the Get command.

```
SANbox (admin) #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n

SANbox (admin) #> quit
>ftp switch_ip_address
user:     images
password: images

ftp>bin
ftp>get dump_support.tgz
    xxxxx bytes sent in xx secs.
ftp> quit
```

The following is an example of the Create Certificate command:

```
SANbox (admin) #> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

Date

Displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax **date**

[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***

Specifies the date – this requires an Admin session. If you omit [MMDDhhmmCCYY], the current date is displayed which does not require an Admin session.

Notes Network Time Protocol (NTP) must be disabled to set the time with the Date command. Enter the Set Setup System command to disable the NTPClientEnabled parameter.

When setting the date and time on a switch that is enabled for SSL connections, the switch time must be within 24 hours of the workstation time. Otherwise, the connection will fail.

Examples The following is an example of the Date command:

```
SANbox #> date
  Mon Apr 07 07:51:24 200x
```

Exit

Closes the Telnet session.

Authority None

Syntax **exit**

Notes You can also enter Control-D to close the Telnet session.

Fcping

NOTE: This command requires the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Verifies a Fibre Channel connection with another switch or a device and reports status.

Authority None

Syntax **fcping destination [address]**
count [number]
timeout [seconds]

Keywords **[address]**

The address of the port or device with which to verify the Fibre Channel connection. [address] can have one of the following formats:

- 6-character hexadecimal device Fibre Channel address (hex). Enter addresses with or without the “0x” prefix.
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxxxx.

count [number]

Number of times given by [number] to repeat the command. If you omit this keyword, the command is repeated once.

timeout [seconds]

Number of seconds given by [seconds] to wait for a response. If you omit this keyword, the switch waits 1 second for a response.

Examples The following is an example of the Fcping command:

```
SANbox #> fcping 970400 count 3
28 bytes from local switch to 0x970400 time = 10 usec
28 bytes from local switch to 0x970400 time = 11 usec
28 bytes from local switch to 0x970400 time = 119 usec
```

Fctrace

NOTE: This command requires the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Displays the path from an initiator device port in the fabric to a target device port in the same zone. To trace the path between two initiator ports, you must disable the I/O StreamGuard feature. Use the Set Config Port command to change the IOStreamGuard parameter.

Path information includes the following:

- Domain IDs
- Incoming port name and physical port number
- Outgoing port name and physical port number

Authority None

Syntax **fctrace [port_source] [port_destination] *[hop_count]***

Keywords **[port_source]**

The Fibre Channel port from to begin the trace. [port_source] can have the following formats:

- 6-character hexadecimal device Fibre Channel address (hex). Enter addresses with or without the “0x” prefix.
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxxxx.

[port_destination]

The Fibre Channel port at which to end the trace. [port_destination] can have the following formats:

- 6-character hexadecimal device Fibre Channel address (hex). Enter addresses with or without the “0x” prefix.
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxxxx.

[hop_count]

Maximum number of hops before stopping the trace. If you omit [hop_count], 20 hops is used.

Examples

The following is an example of the Fctrace command:

```
SANbox#> fctrace 970400 970e00 hops 5

  36 bytes from 0x970400 to 0x970e00, 5 hops max

  Domain  Ingress Port WWN         Port  Egress Port WWN          Port
  ------  ----------------         ----  ---------------          ----
  97      20:04:00:c0:dd:02:cc:2e  4     20:0e:00:c0:dd:02:cc:2e  14
  97      20:0e:00:c0:dd:02:cc:2e  14    20:04:00:c0:dd:02:cc:2e  4
```

Feature

Adds license key features to the switch and displays the license key feature log. To order a license key contact your switch distributor or your authorized reseller. Upgrading a switch is not disruptive, nor does it require a switch reset.

Authority Admin session for Add keyword only

Syntax **feature**

add [license_key]

log

Keywords **add [license_key]**

Adds the feature that corresponds to the value given by [license_key]. [license_key] is case insensitive.

log

Displays a list of installed license key features.

Notes The following license keys are available:

- Enterprise Fabric Suite 2007 is a workstation-based Java® application that provides a graphical user interface for fabric management. This includes Performance View which graphs port performance. Enterprise Fabric Suite 2007 comes with a free 30-day trial license.
- Fabric Security provides for Secure Socket Layer (SSL) and Secure Shell (SSH) connection security, device security using Challenge Handshake Authentication Protocol (CHAP), and remote authentication using a Remote Authentication Dial-In User Service (RADIUS) server.
- SANdoctor provides tools for Fibre Channel connection verification (Fcping command), Fibre Channel route tracing (Fctrace command), and transceiver diagnostic information (Show Media command).
- Port Activation enables additional Fibre Channel ports up to the 20-port maximum.

Examples The following is an example of the Feature Add command:

```
SANbox #> admin start
SANbox (admin) #> feature add 1-LCVXOWUNOJBE6
License upgrade to 20 ports

Do you want to continue with license upgrade procedure? (y/n): [n] y
Alarm Msg:[day mon date time year][A1005.0030][SM][Upgrading Licensed Ports to 20]
```

The following is an example of the Feature Log command:

```
SANbox #> feature log
  Mfg Feature Log:
  ----------------
  Switch Licensed for 8 ports
  Customer Feature Log:
  ---------------------
  1) day month date 19:39:24 year - Switch Licensed for 20 ports
  1-LCVXOWUNOJBE6
```

Firmware Install

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch to activate the firmware. This is disruptive. The command prompts you for the following:

- The file transfer protocol (FTP or TFTP)
- IP address of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

Authority Admin session

Syntax **firmware install**

Examples The following is an example of the Firmware Install command using FTP:

```
SANbox #> admin start
SANbox (admin) #> firmware install
  The switch will be reset.  This process will cause a disruption
  to I/O traffic.
  Continuing with this action will terminate all management sessions,
  including any Telnet sessions. When the firmware activation is complete,
  you may log in to the switch again.

  Do you want to continue? [y/n]: y
      Press 'q' and the ENTER key to abort this command.

  FTP or TFTP     : ftp
  User Account    : johndoe
  IP Address      : 10.0.0.254
  Source Filename : 6.7.00.11_mpc
  About to install image.  Do you want to continue? [y/n] y

Connected to 10.0.0.254 (10.0.0.254).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

The following is an example of the Firmware Install command using TFTP:

```
SANbox #> admin start
SANbox (admin) #> firmware install
  The switch will be reset.  This process will cause a disruption
  to I/O traffic.
  Continuing with this action will terminate all management sessions,
  including any Telnet sessions. When the firmware activation is complete,
  you may log in to the switch again.

  Do you want to continue? [y/n]: y

      Press 'q' and the ENTER key to abort this command.

  FTP or TFTP     : tftp
  IP Address      : 10.0.0.254
  Source Filename : 6.7.00.11_mpc
  About to install image.  Do you want to continue? [y/n] y

Connected to 10.0.0.254 (10.0.0.254).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Group

NOTE: This command requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Creates groups, manages membership within the group, and manages the membership of groups in security sets.

Authority Admin session and a Security Edit session. Refer to the "Security" command on page 13-52 for information about starting a Security Edit session. The List, Members, Securitysets, and Type keywords are available without an Admin session.

Syntax

group
add [group]
copy [group_source] [group_destination]
create [group] *[type]*
delete [group]
edit [group] [member]
list
members [group]
remove [group] [member_list]
rename [group_old] [group_new]
securitysets [group]
type [group]

Keywords add [group]

Initiates an editing session in which to specify a group member and its attributes for the existing group given by [group]. ISL, Port, and MS member attributes are described in Table 13-1, Table 13-2, and Table 13-3 respectively. The group name and group type attributes are read-only fields common to all three tables.

Table 13-1. ISL Group Member Attributes

Attribute	Description
Member	Worldwide name of the switch that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the ISL member. The hash functions are MD5 or SHA-1. If the ISL member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the ISL group member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the ISL group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the ISL group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Binding	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. 0 (zero) specifies no binding.

Table 13-2. Port Group Member Attributes

Attribute	Description
Member	Worldwide port name (WWPN) for the N_Port device that would attach to the switch. A member cannot belong to more than one group. All loop device WWPNs must be included in the group, otherwise the switch port will be downed, and none of the devices will be able to log in.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the Port group member. The hash functions are MD5 or SHA-1. If the Port group member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the Port group member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the Port group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the Port group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

Table 13-3. MS Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch.
CTAuthentication	Common Transport (CT) authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Hash	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Secret	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

copy [group_source] [group_destination]

Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

create [group] *[type]*

Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. [type] can be one of the following:

isl

Configures security for attachments to other switches.

Port

Configures security for attachments to N_Port devices.

ms

Configures security for attachments to N_Port devices that are issuing management server commands.

edit [group] [member]

Initiates an editing session in which to change the attributes of a worldwide name given by [member] in a group given by [group]. Member attributes that can be changed are described in Table 13-4.

Table 13-4. Group Member Attributes

Attribute	Description
Authentication (ISL and Port Groups)	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP).
CTAuthentication (MS Groups)	CT authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Primary Hash (ISL and Port Groups)	The preferred hash function to use to decipher the encrypted Primary Secret sent by the member. The hash functions are MD5 or SHA-1. If the member does not support the Primary Hash, the switch will use the Secondary Hash.
Hash (MS Groups)	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Primary Secret (ISL and Port Groups)	Hexadecimal string that is encrypted by the Primary Hash for authentication with the member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash (ISL and Port Groups)	Hash function to use to decipher the encrypted Secondary Secret sent by the group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret (ISL and Port Groups)	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secret (MS Groups)	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

Table 13-4. Group Member Attributes (Continued)

Attribute	Description
Binding (ISL Groups)	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. 0 (zero) specifies no binding.

list

Displays a list of all groups and the security sets of which they are members. This keyword is available without an Admin session.

members [group]

Displays all members of the group given by [group]. This keyword is available without an Admin session.

remove [group] [member_list]

Remove the port/device worldwide name given by [member] from the group given by [group]. Use a <space> to delimit multiple member names in [member_list]

rename [group_old] [group_new]

Renames the group given by [group_old] to the group given by [group_new].

securitysets [group]

Displays the list of security sets of which the group given by [group] is a member. This keyword is available without an Admin session.

type [group]

Displays the group type for the group given by [group]. This keyword is available without an Admin session.

Notes

Primary and secondary secrets are not included in a switch configuration backup. Therefore, after restoring a switch configuration, you must re-enter the primary and secondary secrets. Otherwise, the switch will isolate because of an authentication failure.

Refer to the “Securityset” command on page 13-56 for information about managing groups in security sets.

Examples

The following is an example of the Group Add command:

```
SANbox #> admin start
SANbox (admin) #> security edit
SANbox (admin-security) #> group add Group_1
  A list of attributes with formatting and default values will follow
  Enter a new value or simply press the ENTER key to accept the current value
  with exception of the Group Member WWN field which is mandatory.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name       Group_1
  Group Type       ISL
  Member          (WWN)                          [00:00:00:00:00:00:00:00]
  Authentication  (None / Chap)                  [None                    ]
  PrimaryHash     (MD5 / SHA-1)                  [MD5                     ]
  PrimarySecret   (32 hex or 16 ASCII char value)[                        ]
  SecondaryHash   (MD5 / SHA-1 / None)           [None                    ]
  SecondarySecret (40 hex or 20 ASCII char value)[                        ]
  Binding         (domain ID 1-239, 0=None)      [0                       ]


  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group Edit command:

```
SANbox #> admin start
SANbox (admin) #> security edit
SANbox (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Group Name        g1
  Group Type        ISL
  Group Member      10:00:00:c0:dd:00:90:a3
  Authentication    (None / Chap)                  [None]  chap
  PrimaryHash       (MD5 / SHA-1)                  [MD5 ]  sha-1
  PrimarySecret     (40 hex or 20 ASCII char value)[    ]  12345678901234567890
  SecondaryHash     (MD5 / SHA-1 / None)           [None]  md5
  SecondarySecret   (32 hex or 16 ASCII char value)[    ]  1234567890123456
  Binding           (domain ID 1-239, 0=None)      [3   ]


  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group List command:

```
SANbox #> group list
  Group       SecuritySet
  -----       -----------
  group1 (ISL)
              alpha
  group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
SANbox #> group members group_1
  Current list of members for Group: group_1
  ----------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

Hardreset

Resets the switch and performs a power-on self test. This reset disrupts I/O traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, refer to the “Set Log” command on page 13-76.

Authority Admin session

Syntax **hardreset**

Notes To reset the switch without a power-on self test, refer to the “Reset” command on page 13-43.

To reset the switch without disrupting traffic, refer to the “Hotreset” command on page 13-33.

Help

Displays a brief description of the specified command, its keywords, and usage.

Authority None

Syntax **help *[command] [keyword]***

Keywords ***[command]***

Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands.

[keyword]

Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all

Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Config command:

```
SANbox #> help config
config CONFIG_OPTIONS
The config command operates on configurations.

  Usage: config   { activate | backup   | cancel   | copy     | delete   |
                    edit     | list     | restore  | save }
```

The following is an example of the Help Config Edit command:

```
SANbox #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

History

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax **history**

Notes Use the History command to provide context for the ! command:

- Enter ![command_string] to re-execute the most recent command that matches [command_string].
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
SANbox #> history
   1 show switch
   2 date
   3 help set
   4 history

SANbox #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:

  Usage: set   { alarm     | beacon    | config    | log       | pagebreak |
                 port      | setup     | switch }
```

Hotreset

Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the event log. After the pending firmware is activated, the configuration is recovered. This process may take a few minutes. To save the event log to a file before resetting, enter the Set Log Archive command.

Authority Admin session

Syntax **hotreset**

Notes

- You can load and activate version 6.7.x firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices under the following conditions:
  - The current firmware version permits the installation and non-disruptive activation of 6.7 firmware. Refer to the 6.7 Firmware Release Notes for previous compatible firmware versions.
  - No changes are being made to switches in the fabric including installing firmware, powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
  - No port on the switch is in the diagnostic state.
  - No zoning changes are being made on the switch.
  - No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.
- Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, Enterprise Fabric Suite 2007 sessions reconnect automatically. However, CLI and SSH sessions must be restarted manually.
- This command clears the event log and all counters.

Image

Manages and installs switch firmware.

Authority Admin session

Syntax **image**

cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
install
list
tftp [ip_address] [file_source] [file_destination]
unpack [file]

Keywords **cleanup**

Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]

Retrieves image file given by [file_source] using FTP and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the host IP address given by [Ip_address]. If an account name needs a password to access the FTP server, the system will prompt you for it.

install

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch to activate the firmware. This is disruptive. The command prompts you for the following:

- File transfer protocol (FTP or TFTP)
- IP address of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

list

Displays the list of image files that reside on the switch.

tftp [ip_address] [file_source] [file_destination]

Retrieves image file given by [file_source] using TFTP and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the host IP address given by [Ip_address].

unpack [file]

Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes

To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

To install firmware when the management workstation has an FTP server, use the Image Install command or the Firmware Install command.

Examples

The following is an example of the Image Install command:

```
SANbox #> admin start
SANbox (admin) #> image install
  Warning: Installing new firmware requires a switch reset.

  Continuing with this action will terminate all management sessions,
  including any Telnet sessions. When the firmware activation is complete,
  you may log in to the switch again.

  Do you want to continue? [y/n]: y

      Press 'q' and the ENTER key to abort this command.

  FTP or TFTP     : ftp
  User Account    : johndoe
  IP Address      : 10.0.0.254
  Source Filename : 6.7.00.11_mpc
  About to install image.  Do you want to continue? [y/n] y

Connected to 10.0.0.254 (10.0.0.254).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

The following is an example of the Image Fetch and Image Unpack commands:

```
SANbox (admin) #> image fetch johndoe 10.0.0.254 6.7.00.11_mpc
>ftp 10.0.0.254
user:johndoe
password: ********
ftp>bin
ftp>put 6.7.00.11_mpc
ftp>quit
SANbox (admin) $>image list
SANbox (admin) $>image unpack 6.7.00.11_mpc
Image unpack command result: Passed
```

Lip

Reinitializes the specified loop port.

Authority Admin session

Syntax **lip [port_number]**

Keywords **[port_number]**

The number of the port to be reinitialized. Ports are numbered beginning with 0.

Examples The following is an example of the Lip command:

```
SANbox (admin) #> lip 2
```

Logout

Closes the Telnet session.

Authority None

Syntax **logout**

Notes You can also enter Control-D to close the Telnet session.

Passwd

Changes a user account's password.

Authority Admin account name and an Admin session to change another account's password; You can change you own password without an Admin session.

Syntax **passwd [account_name]**

Keywords **[account_name]**

The user account name. To change the password for an account name other than your own, you must open an Admin session with the account name Admin. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
SANbox #> admin start
SANbox (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (8-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Ping

Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax **ping [ip_address]**

Keywords **[ip_address]**

The IP address of the switch to query. Broadcast IP addresses, such as 255.255.255.255, are not valid.

Examples The following is an example of a successful Ping command:

```
SANbox #> ping 10.20.11.57
  Ping command issued. Waiting for response...
SANbox #>
  Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
SANbox #> ping 10.20.11.57
  Ping command issued. Waiting for response...
  No response from 10.20.11.57. Unreachable.
```

Ps

Displays current system process information.

Authority None

Syntax **ps**

Examples The following is an example of the Ps command:

```
SANbox #> ps
PID  PPID %CPU     TIME     ELAPSED COMMAND
338   327  0.0 00:00:00  3-01:18:35 cns
339   327  0.0 00:00:01  3-01:18:35 ens
340   327  0.0 00:00:21  3-01:18:35 dlog
341   327  0.1 00:05:35  3-01:18:35 ds
342   327  0.2 00:11:29  3-01:18:35 mgmtApp
343   327  0.0 00:00:04  3-01:18:35 fc2
344   327  0.0 00:02:16  3-01:18:35 nserver
345   327  0.0 00:02:44  3-01:18:35 mserver
346   327  0.8 00:35:12  3-01:18:35 util
347   327  0.0 00:00:29  3-01:18:35 snmpservicepath
348   327  0.0 00:02:46  3-01:18:34 eport
349   327  0.0 00:00:21  3-01:18:34 PortApp
350   327  5.6 04:08:24  3-01:18:34 port_mon
351   327  0.0 00:01:38  3-01:18:34 zoning
352   327  0.0 00:00:01  3-01:18:34 diagApp
404   327  0.0 00:00:04  3-01:18:27 snmpd
405   327  0.0 00:00:02  3-01:18:27 snmpmain
406   405  0.0 00:00:00  3-01:18:26 snmpmain
```

Quit

Closes the Telnet session.

Authority None

Syntax **quit**

Notes You can also enter Control-D to close the Telnet session.

Reset

Resets the switch configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority Admin session

Syntax **reset**

config *[config_name]*
factory
port [port_list]
radius
security
services
snmp
switch (default)
system
zoning

Keywords **config *[config_name]***

Resets the configuration given by [config_name] to the factory default values for switch, port, port threshold alarm, and zoning configuration as described in Table 13-5 through Table 13-13. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration for the changes to take effect.

factory

Resets switch configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, security configuration, RADIUS configuration, switch services configuration, and zoning to the factory default values as described in Table 13-5 through Table 13-13. The switch configuration is activated automatically.

NOTE:
- Because this keyword changes network parameters, the workstation could lose communication with the switch and release the Admin session.
- This keyword does not affect installed license keys.

port [port_list]

Reinitializes one or more ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15.

radius

Resets the RADIUS configuration to the default values as described in Table 13-10.

security

Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged.

services

Resets the switch services configuration to the default values as described in Table 13-11.

snmp

Resets the SNMP configuration settings to the factory default values. Refer to Table 13-9 for SNMP configuration default values.

switch

Resets the switch without a power-on self test. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware.
- Closes all management sessions.
- Clears the event log. To save the event log before resetting, refer to the "Set Log" command on page 13-76.

To reset the switch with a power-on self test, refer to the "Hardreset" command on page 13-30. To reset the switch without disrupting traffic, refer to the "Hotreset" command on page 13-33.

NOTE: The following files are deleted from the switch during a switch reset:

- Firmware image files that have not been unpacked
- Configuration backup files
- Support files

system

Resets the system configuration settings to the factory default values as described in Table 13-12.

NOTE:

- Because this keyword changes network parameters, the workstation could lose communication with the switch.
- This keyword does not affect installed license keys.

zoning

Clears the zoning database and deactivates the active zone set. The zoning configuration parameters (InteropAutoSave, DefaultZone, DiscardInactive) remain unchanged. Refer to Table 13-8 for information about the zoning configuration parameters.

Notes

The following tables specify the various factory default settings:

Enter the Show Config Switch command to display switch configuration values.

Table 13-5. Switch Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
DefaultDomain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	SANbox
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	Config Default
InteropMode	Standard

Enter the Show Config Port command to display port configuration values.

Table 13-6. Port Configuration Defaults

Parameter	1/2/4-Gbps Port Defaults	10-Gbps Port Defaults
Admin State	Online	Online
Link Speed	Auto	10-Gbps
Port Type	GL	G
Symbolic Name	Portn, where n is the port number	10G-n, where n is the port number
ALFairness	False	N/A
DeviceScanEnabled	True	True
ForceOfflineRSCN	False	False
ARB_FF	False	N/A
InteropCredit	0	0
ExtCredit	0	N/A
FANEnable	True	N/A
AutoPerfTuning	True	True
LCFEnable	False	False
MFSEnable	False	False
MSEnable	True	False
NoClose	False	N/A
IOStreamGuard	Auto	Auto
VIEnable	False	False
PDISCPingEnable	True	N/A

Enter Show Config Threshold command to display threshold alarm configuration values.

Table 13-7. Port Threshold Alarm Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled	True
■ RisingTrigger	25
■ FallingTrigger	1
■ SampleWindow	10
DecodeErrorsMonitoringEnabled	True
■ RisingTrigger	25
■ FallingTrigger	0
■ SampleWindow	10
ISLMonitoringEnabled	True
■ RisingTrigger	2
■ FallingTrigger	0
■ SampleWindow	10
LoginMonitoringEnabled	True
■ RisingTrigger	5
■ FallingTrigger	1
■ SampleWindow	10
LogoutMonitoringEnabled	True
■ RisingTrigger	5
■ FallingTrigger	1
■ SampleWindow	10
LOSMonitoringEnabled	True
■ RisingTrigger	100
■ FallingTrigger	5
■ SampleWindow	10

Enter the Show Config Zoning command to display zoning configuration values.

Table 13-8. Zoning Configuration Defaults

Parameter	Default
InteropAutoSave	True
DefaultZone	True
DiscardInactive	False

Enter the Show Setup SNMP command to display SNMP configuration values.

Table 13-9. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	SANbox 5000 Series FC Switch
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.17 (SANbox 5200) 1.3.6.1.4.1.1663.1.1.1.1.30 (SANbox 5202) 1.3.6.1.4.1.1663.1.1.1.1.23 (SANbox 5600 1.3.6.1.4.1.1663.1.1.1.1.24 (SANbox 5602)
AuthFailureTrap	False
ProxyEnabled	True

Enter the Show Setup Radius command to display RADIUS configuration values.

Table 13-10. RADIUS Configuration Defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	1
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds
Retries	0
SignPackets	False

Enter the Show Setup Services command to display switch service configuration values.

Table 13-11. Services Configuration Defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True.
MgmtServerEnabled	False

Enter the Show Setup System command to display system configuration values.

Table 13-12. System Configuration Defaults

Parameter	Default
Ethernet Network Enable	True
Ethernet Network Discovery	Static
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Admin Timeout	30 minutes
InactivityTimeout	0
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Enter the Show Config Security command to display security configuration values.

Table 13-13. Security Configuration Defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	False
PortBindingEnabled	False

Security

NOTE: This command requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Opens a Security Edit session in which to manage the security database on a switch. Refer to the "Group" command on page 13-22 and the "Securityset" command on page 13-56.

Authority Admin session. The keywords Active, History, Limits, and List are available without an Admin session.

Syntax

security
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active

Displays the active security set, its groups, and group members. This keyword does not require an Admin session.

cancel

Closes a Security Edit session without saving changes. Use the Edit keyword to open a Security Edit session.

clear

Clears all inactive security sets from the volatile edit copy of the security database. This keyword does not affect the non-volatile security database. However, if you enter the Security Clear command followed by the Security Save command, the non-volatile security database will be cleared from the switch.

NOTE: The preferred method for clearing the security database from the switch is the Reset Security command.

edit

Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To close a Security Edit session and save changes, enter the Security Save command. To close a Security Edit session without saving changes, enter the Security Cancel command.

history

Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This keyword does not require an Admin session.

limits

Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This keyword does not require an Admin session.

list

Displays all security sets, groups, and group members in the security database. This keyword does not require an Admin session.

restore

Restores the volatile security database with the contents of the non-volatile security database. If the AutoSave parameter is False, you can use this keyword to revert changes to the volatile security database that were propagated from another switch in the fabric through security set activation or merging fabrics. Refer to Table 13-13 for information about the AutoSave parameter.

save

Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. Refer to the “Securityset” command on page 13-56 for information about activating a security set.

Examples

The following is an example of the Security Active command:

```
SANbox #> security active
  Active Security Information

  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

The following is an example of the Security History command:

```
SANbox #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  day month date time year
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           day month date time year
  Database Checksum                   00007558
```

The following is an example of the Security Limits command:

```
SANbox #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

The following is an example of the Security List command:

```
SANbox #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

Securityset

NOTE: This command requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Manages security sets in the security database.

Authority Admin session and a Security Edit session. Refer to the "Security" command on page 13-52 for information about starting a Security Edit session. The Active, Groups, and List keywords are available without an Admin session. You must close the Security Edit session before using the Activate and Deactivate keywords.

Syntax **securityset**

activate [security_set]
active
add [security_set] [group_list]
copy [security_set_source] [security_set_destination]
create [security_set]
deactivate
delete [security_set]
groups [security_set]
list
remove [security_set] [group]
rename [security_set_old] [security_set_new]

Keywords **activate [security_set]**

Activates the security set given by [security_set]. This keyword deactivates the active security set. Close the Security Edit session using the Security Save or Security Cancel command before using this keyword.

active

Displays the name of the active security set. This keyword is available to without an Admin session.

add [security_set] [group_list]

Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]

Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]

Creates the security set with the name given by [security_set]. A security set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 4 security sets.

deactivate

Deactivates the active security set. Close the Security Edit session before using this keyword.

delete [security_set]

Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]

Displays all groups that are members of the security set given by [security_set]. This keyword is available without an Admin session.

list

Displays a list of all security sets. This keyword is available without an Admin session.

remove [security_set] [group]

Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]

Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes

Refer to the “Group” command on page 13-22 for information about creating and managing groups.

Examples

The following is an example of the Securityset Active command

```
SANbox #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet alpha
  LastActivatedBy  Remote
  LastActivatedOn  day month date time year
```

The following is an example of the Securityset Groups command

```
SANbox #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  --------------------------------------
  group1 (ISL)
  group2 (Port)
```

The following is an example of the Securityset List command

```
SANbox #> securityset list
Current list of SecuritySets
---------------------------
  alpha
  beta
```

Set Alarm

Controls the display of alarms in the session output stream or clears the alarm log.

Authority Admin session for the Clear keyword. Otherwise, none.

Syntax **set alarm [option]**

Keywords **[option]**

[option] can be one of the following:

clear

Clears the alarm log history. This value requires an Admin session.

on

Enables the display of alarms in the session output stream.

off

Disables the display of alarms in the session output stream. Disabling the display of alarms in the output stream allows command scripts to run without interruption.

Examples The following is an example of the Set Alarm command:

```
SANbox #> set alarm on
```

Set Beacon

Enables or disables the flashing of the Logged-In LEDs for the purpose of locating a switch.

Authority None

Syntax **set beacon [state]**

Keywords **[state]**

[state] can be one of the following:

on

Enables the flashing beacon.

off

Disables the flashing beacon.

Examples The following is an example of the Set Beacon command:

```
SANbox #> set beacon on
```

Set Config Port

Sets the port configuration parameters for one or more ports. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority Admin session and a Config Edit session

Syntax **set config port *[port_number]***

or

set config ports *[port_number]*

Keywords **port *[port_number]***

Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration for one port, or “qq” to end the configuration for all ports. Table 13-14 describes the port configuration parameters.

ports *[port_number]*

Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration. Table 13-14 describes the port configuration parameters.

Table 13-14. Port Configuration Parameters

Parameter	Description
AdminState	Port administrative state: ■ Online – Activates and prepares the port to send data. This is the default. ■ Offline – Prevents the port from receiving signal and accepting a device login. ■ Diagnostics – Prepares the port for testing and prevents the port from accepting a device login. ■ Down – Disables the port by removing power from the port lasers.
LinkSpeed	Transmission speed: ■ 1/2/4-Gbps Ports: 1-Gbps, 2 Gbps, 4-Gbps, or Auto. The default is Auto. ■ 10-Gbps Ports: 10-Gbps or Auto. The default is Auto.

Table 13-14. Port Configuration Parameters (Continued)

Parameter	Description
PortType	Port types: ■ 1/2/4-Gbps Ports: GL, G, F, FL, Donor. The default is GL. ■ 10-Gbps Ports: GL, G, F, FL, Donor. The default is GL. The Donor port type disables the port and makes the buffer credits available to other ports. Refer to the ExtCredit port configuration parameter.
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Port n where n is the port number.
ALFairness (1/2/4-Gbps ports only)	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default is unchanged. Default buffer-to-buffer credits are 16 per port. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.

Table 13-14. Port Configuration Parameters (Continued)

Parameter	Description
AutoPerfTuning	Automatic performance tuning for FL_Ports only. The default is True. ■ If AutoPerfTuning is enabled (True) and the port is an FL_Port, MFSEnable is automatically enabled. LCFEnable and VIEnable are overridden to False. ■ If AutoPerfTuning is disabled (False), MFSEnable, LCFEnable, and VIEnable retain their original values.
LCFEnable	Link control frame preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. This parameter appears only if AutoPerfTuning is False. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is false. Enabling MFSEnable disables LCFEnable and VIEnable.
VIEnable	Virtual Interface (VI) preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
IOStreamGuard	I/O Stream Guard. Enables or disables the suppression of RSCN messages. IOStreamGuard can have the following values: ■ Enable – Suppresses the reception of RSCN messages from other ports for which IOStreamGuard is enabled. ■ Disable – Allows free transmission and reception of RSCN messages. ■ Auto – Suppresses the reception of RSCN messages when the port is connected to an initiator device with a QLogic HBA. For older QLogic HBAs, such as the QLA2200, the DeviceScanEnabled parameter must also be enabled. The default is Auto.

Table 13-14. Port Configuration Parameters (Continued)

Parameter	Description
PDISCPingEnable (1/2/4-Gbps ports only)	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

Examples

The following is an example of the Set Config Port command:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------

  AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down)       [Online]
  LinkSpeed        (1=1Gb/s, 2=2Gb/s, 4=4Gb/s, A=Auto)                [Auto  ]
  PortType         (GL / G / F / FL / Donor)                          [GL    ]
  SymPortName      (string, max=32 chars)                             [Port1 ]
  ALFairness       (True / False)                                     [False ]
  DeviceScanEnable (True / False)                                     [True  ]
  ForceOfflineRSCN (True / False)                                     [False ]
  ARB_FF           (True / False)                                     [False ]
  InteropCredit    (decimal value, 0-255)                             [0     ]
  ExtCredit        (dec value, increments of 15, non-loop only)       [0     ]
  FANEnable        (True / False)                                     [True  ]
  AutoPerfTuning   (True / False)                                     [False ]
  LCFEnable        (True / False)                                     [False ]
  MFSEnable        (True / False)                                     [False ]
  VIEnable         (True / False)                                     [False ]
  MSEnable         (True / False)                                     [True  ]
  NoClose          (True / False)                                     [False ]
  IOStreamGuard    (Enable / Disable / Auto)                          [Disable]
  PDISCPingEnable  (True / False)                                     [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Port command for a 10-Gbps port:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config port 16

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  16
  ------------------------

AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online  ]
LinkSpeed        (10=10Gb/s)                                  [10Gb/s  ]
PortType         (G / F)                                      [G       ]
SymPortName      (string, max=32 chars)                       [10G-16  ]
DeviceScanEnable (True / False)                               [True    ]
ForceOfflineRSCN (True / False)                               [False   ]
AutoPerfTuning   (True / False)                               [Fales   ]
LCFEnable        (True / False)                               [False   ]
MFSEnable        (True / False)                               [False   ]
VIEnable         (True / False)                               [False   ]
MSEnable         (True / False)                               [True    ]
IOStreamGuard    (Enable / Disable / Auto)                    [Disabled]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Config Security

NOTE: This command requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Configures the security database for the automatic saving of changes to the active security set and fabric binding. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority

Admin session and a Config Edit session

Syntax

set config security

This command initiates an editing session in which to change the security database configuration. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table 13-15 describes the security configuration parameters.

Table 13-15. Security Configuration Parameters

Parameter	Description
AutoSave	Enables (True) or disables (False) the saving of changes to active security set in the switch’s permanent memory. The default is True.
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding on all switches in the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

Examples

The following is an example of the Set Config Security command:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config security
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
```

```
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

FabricBindingEnabled  (True / False)     [False]
AutoSave              (True / False)     [True ]

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

Set Config Security Portbinding

Configures port binding.

Authority Admin session and a Config Edit session

Syntax **set config security portbinding [port_number]**

Keywords **[port_number]**

Initiates an editing session in which to change the port binding configuration for the port given by [port_number]. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table 13-16 describes the Set Config Security Port parameters.

Table 13-16. Port Binding Configuration Parameters

Parameter	Description
PortBindingEnabled	Enables (True) or disables (False) port binding for the port given by [port_number].
WWN	Worldwide port name for the port/device that is allowed to connect to the port given by [port_number].

Examples The following is an example of the Set Config Security Portbinding command:

```
SANbox #> admin start
SANbox (admin) config edit
SANbox (admin-config) #> set config security portbinding 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PortBindingEnabled (True / False)[False] true
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f9
  WWN                (N=None / WWN)[None ] 10:00:00:c0:dd:00:b9:f8
  WWN                (N=None / WWN)[None ] n

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Config Switch

Sets the switch configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority Admin session and a Config Edit session

Syntax **set config switch**

This command initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table 13-17 describes the switch configuration parameters.

Table 13-17. Switch Configuration Parameters

Parameter	Description
AdminState	Switch administrative state. ■ Online – Activates and prepares the ports to send data. This is the default. ■ Offline – Prevents the ports from receiving signal and accepting a device login. ■ Diagnostics – Prepares the ports for testing and prevents the ports from accepting a device login. ■ Down – Disables the ports by removing power from the port lasers.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information. The default is True.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.

Table 13-17. Switch Configuration Parameters (Continued)

Parameter	Description
SymbolicName	Descriptive name for the switch. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is SANbox.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Config Default.
InteropMode	Standard, FC-SW-2 compliant interoperability.

Examples

The following is an example of the Set Config Switch command:

```
SANbox #> admin start
SANbox (admin) #> config edit
SANbox (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState          (1=Online, 2=Offline, 3=Diagnostics)   [Online        ]
  BroadcastEnabled    (True / False)                         [True          ]
  InbandEnabled       (True / False)                         [True          ]
  FDMIEnabled         (True / False)                         [True          ]
  FDMIEntries         (decimal value, 0-1000)                [1000          ]
  DefaultDomainID     (decimal value, 1-239)                 [2             ]
  DomainIDLock        (True / False)                         [False         ]
  SymbolicName        (string, max=32 chars)                 [SANbox        ]
  R_A_TOV             (decimal value, 100-100000 msec)       [10000         ]
  E_D_TOV             (decimal value, 10-20000 msec)         [2000          ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]
  InteropMode         (0=Standard, 1=Interop_1)              [Standard      ]
```

Set Config Threshold

Sets the port alarm threshold parameters by which the switch monitors port performance and generates alarms. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority Admin session and a Config Edit session

Syntax **set config threshold**

Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table 13-18 describes the port alarm threshold parameters.

Table 13-18. Port Alarm Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: ■ CRC errors ■ Decode errors ■ ISL connection count ■ Device login errors ■ Device logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The switch will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The time in seconds in which to count events.

Notes The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Examples The following is an example of the Set Config Threshold command:

```
SANbox #> admin start
SANbox  (admin) #> config edit
SANbox (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled     (True / False)              [False     ]
CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
ISLMonitoringEnabled           (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [2         ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LoginMonitoringEnabled         (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
LogoutMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]
 LOSMonitoringEnabled           (True / False)             [True      ]
  RisingTrigger                (decimal value, 1-1000)     [100       ]
  FallingTrigger               (decimal value, 0-1000)     [5         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

Finished configuring attributes.
This configuration must be saved (see config save command) and activated (see
config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

Set Config Zoning

Configures the zoning database. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command.

Authority Admin session and a Config Edit session

Syntax **set config zoning**

Initiates an editing session in which to change the zoning database configuration. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table 13-19. Zoning Configuration Parameters

Parameter	Description
InteropAutoSave	Enables (True) or disables (False) the saving of changes to active zone set in the switch's non-volatile zoning database.The default is True. Disabling the Autosave parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the InteropAutoSave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the InteropAutoSave parameter should be enabled in a production environment.
DefaultZone	Enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set. The default is True.
DiscardInactive	Enables (True) or disables (False) the discarding of all inactive zone sets from that zoning database. Inactive zone sets are all zone sets except the active zone set. The default is False.

Examples

The following is an example of the Set Config Zoning command.

```
SANbox #> admin start
SANbox (admin) #> config edit
   The config named default is being edited.
SANbox (admin-config) #> set config zoning
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

  InteropAutoSave      (True / False)  [True ]
  DefaultZone          (True / False)  [True ]
  DiscardInactive      (True / False)  [False]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Log

Specifies the events to record in the event log and display on the screen. You determine what events to record in the switch event log using the Component, Level, and Port keywords. You determine what events are automatically displayed on the screen using the Display keyword. Alarms are always displayed on the screen.

Authority Admin session

Syntax **set log**

archive
clear
component [filter_list]
display [filter]
level [filter]
port [port_list]
restore
save
start (default)
stop

Keywords **archive**

Collects all log entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear

Clears all log entries.

component [filter_list]

Specifies one or more components given by [filter_list] to monitor for events. A component is a firmware module that is responsible for a particular portion of switch operation. Use a <space> to delimit values in the list. [filter_list] can be one or more of the following:

All

Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Eport

Monitors all E_Ports.

Mgmtserver

Monitors management server status.

Nameserver

Monitors name server status.

None

Monitor none of the component events.

Port

Monitors all port events.

SNMP

Monitors all SNMP events.

Switch

Monitors switch management events.

Zoning

Monitors zoning conflict events.

display [filter]

Specifies the log events to automatically display on the screen according to the event severity levels given by [filter]. [filter] can be one of the following values:

Critical

Critical severity level events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn

Warning severity level events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info

Informative severity level events. The informative level describes routine events associated with a normal fabric.

None

Specifies no severity levels for display on the screen.

level [filter]

Specifies the severity level given by [filter] to use in monitoring and logging events for the specified components or ports. [filter] can be one of the following values:

Critical

Monitors critical events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action. This is the default severity level.

Warn

Monitors warning and critical events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info

Monitors informative, warning, and critical events. The informative level describes routine events associated with a normal fabric.

NOTE: Logging events at the Info severity level can deplete switch resources because of the high volume of events.

None

Monitors none of the severity levels.

port [port_list]

Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]

Specifies the port or ports to monitor. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15.

All

Specifies all ports.

None

Disables monitoring on all ports.

restore

Restores and saves the port, component, and level settings to the default values.

save

Saves the log settings for the component, severity level, port, and display level. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start

Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop

Stops logging of events.

Notes

In addition to critical, warn, and informative severity levels, the highest event severity level is alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen.

Set Pagebreak

Specifies how much information is displayed on the screen at a time. This command is useful for disabling pagebreaks to allow command scripts to run without interruption.

Authority None

Syntax **pagebreak [state]**

Keywords **[state]**

[state] can be one of the following:

on

Limits the display of information to 20 lines at a time. The page break function affects the following commands:

- Alias (List, Members)
- Show (Alarm, Log)
- Zone (List, Members)
- Zoneset (List, Zones)
- Zoning (Active, List)

off

Allows continuous display of information without a break. This is the default.

Examples

The following is an example of the Set Pagebreak command:

```
SANbox #> set pagebreak on
SANbox #> zone list

  Zone        ZoneSet
  ----        -------
  Zone1
              alpha
              beta

  Zone2
              delta
              echo

  Zone3
              sierra
              tango

  Zone4
              gamma
              delta

         Press any key to continue, 'q' to quit ...
```

Set Port

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin session

Syntax

set port clear

or

set port [port_number]

bypass [alpa]

clear

enable

speed [transmission_speed]

state [state]

Keywords

[port_number]

Specifies the port. Ports are numbered beginning with 0.

bypass [alpa]

Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear

Clears the counters on all ports or the port given by [port_number].

enable

Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]

Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s

One gigabit per second.

2Gb/s

Two gigabits per second.

4Gb/s

Four gigabits per second.

10Gb/s

Ten gigabits per second. This applies only to ports 16–19.

Auto

The port speed is automatically detected.

state [state]

Specifies one of the following administrative states for the specified port:

Online

Activates and prepares the port to send data.

Offline

Prevents the port from receiving signal and accepting a device login.

Diagnostics

Prepares the port for testing and prevents the port from accepting a device login.

Down

Disables the port by removing power from the port lasers.

Set Setup Radius

NOTE: This command requires the Fabric Security license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller. Use the Feature command to install a license key.

Configures RADIUS servers on the switch.

Authority Admin session

Syntax **set setup radius**

Prompts you in a line-by-line fashion to configure RADIUS servers for user account and device authentication. Table 13-20 describes the RADIUS server configuration fields.

Table 13-20. RADIUS Service Settings

Entry	Description
DeviceAuthOrder	Authenticator priority for devices: ■ Local: Authenticate devices using only the local security database. This is the default. ■ Radius: Authenticate devices using only the security database on the RADIUS server. ■ RadiusLocal: Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
UserAuthOrder	Authenticator priority for user accounts: ■ Local: Authenticate users using only the local security database. This is the default. ■ Radius: Authenticate users using only the security database on the RADIUS server. ■ RadiusLocal: Authenticate users using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
TotalServers	Number of RADIUS servers to configure during this session. Setting TotalServers to 0 disables all RADIUS authentication. The default is 0.
ServerIPAddress	IP address of the RADIUS server. The default is 10.0.0.1.
ServerUDPPort	User Datagram Protocol (UDP) port number on the RADIUS server. The default is 1812.

Table 13-20. RADIUS Service Settings (Continued)

Entry	Description
DeviceAuthServer	Enable (True) or disable (False) this server for device authentication. The default is False.
UserAuthServer	Enable (True) or disable (False) this server for user account authentication. A user authentication RADIUS server requires a secure management connection (SSL). The default is True.
AccountingServer	Enable (True) or disable (False) this server for auditing of activity during a user session. When enabled, user activity is audited whether UserAuthServer is enabled or not.The default is False. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).
Timeout	Number of seconds to wait to receive a response from the RADIUS server before timing out. The default is 2.
Retries	Number of retries after the first attempt to establish communication with the RADIUS server fails. The default is 0.
SignPackets	Enable (True) or disable (False) the use of sign packets to protect the RADIUS server packet integrity. The default is False.
Secret	22-byte ASCII string used as a password for authentication purposes between the switch and the RADIUS server.

Examples

The following is an example of the Set Setup RADIUS command:

```
SANbox (admin) #> set setup radius
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the attributes
  for the server being processed, press 'q' or 'Q' and the ENTER key to do so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to so do.

  DeviceAuthOrder   (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  UserAuthOrder     (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  TotalServers      (decimal value, 0-5)               [1    ]

  Server: 1
  ServerIPAddress   (dot-notated IP Address)         [10.20.11.8]
  ServerUDPPort     (decimal value)                  [1812      ]
  DeviceAuthServer  (True / False)                   [True      ]
  UserAuthServer    (True / False)                   [True      ]
  AccountingServer  (True / False)                   [False     ]
  Timeout           (decimal value, 10-30 secs)      [10        ]
  Retries           (decimal value, 1-3, 0=None)     [0         ]
  SignPackets       (True / False)                   [False     ]
  Secret            (1-63 characters, recommend 22+) [**********]
  Do you want to save and activate this radius setup? (y/n): [n]
```

Set Setup Services

Configures services on the switch.

Authority Admin session

Syntax **set setup services**

Prompts you in a line-by-line fashion to enable or disable switch services. Table 13-21 describes the switch service parameters. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

NOTE: Use caution when disabling TelnetEnabled and GUIMgmtEnabled; it is possible to disable all Ethernet access to the switch.

Table 13-21. Switch Services Settings

Entry	Description
TelnetEnabled	Enables (True) or disables (False) the ability to manage the switch over a Telnet connection. Disabling this service is not recommended. The default is True.
SSHEnabled	Enables (True) or disables (False) Secure Shell (SSH) connections to the switch. SSH secures the remote connection to the switch. To establish a secure remote connection, your workstation must use an SSH client. The default is False. The SSH service requires the Fabric Security license key To purchase a license key, contact your authorized maintenance provider or authorized reseller.
GUIMgmtEnabled	Enables (True) or disables (False) out-of-band management of the switch with Enterprise Fabric Suite 2007, the Application Programming Interface, SNMP, and SMI-S. If this service is disabled, the switch can only be managed inband or through the serial port. The default is True.

Table 13-21. Switch Services Settings (Continued)

Entry	Description
SSLEnabled	Enables (True) or disables (False) secure SSL connections for management applications including Enterprise Fabric Suite 2007, QuickTools, Application Programming Interface, and SMI-S. The default is False. ■ The SSL service requires the Fabric Security license key. ■ To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. ■ This service must be enabled to authenticate users through a RADIUS server. ■ Enabling SSL automatically creates a security certificate on the switch. ■ To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.
EmbeddedGUIEnabled	Enables (True) or disables (False) the QuickTools embedded switch management application. QuickTools enables you to point at a switch with an internet browser and manage the switch. This parameter is the master control for the Set Setup System command parameter, EmbeddedGUIEnabled. The default is True.
SNMPEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). This parameter is the master control for the Set Setup SNMP command parameter, SNMPEnabled. The default is True.
NTPEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) which allows the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is False. This parameter is the master control for the Set Setup System command parameter, NTPClientEnabled. The default is False.
CIMEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use SMI-S.
FTPEnabled	Enables (True) or disables (False) the File Transfer Protocol (FTP) for transferring files rapidly between the workstation and the switch. The default is True.

Table 13-21. Switch Services Settings (Continued)

Entry	Description
MgmtServerEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use GS-3 Management Server (MS). This parameter is the master control for the Set Config Port command parameter, MSEnable. The default is True.

Examples

The following is an example of the Set Setup Services command:

```
SANbox #> admin start
SANbox (admin) #> set setup services

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  PLEASE NOTE:
  -----------
  * Further configuration may be required after enabling a service.

  * If services are disabled, the connection to the switch may be lost.

  * When enabling SSL, please verify that the date/time settings
    on this switch and the workstation from where the SSL connection
    will be started match, and then a new certificate may need to be
    created to ensure a secure connection to this switch.

  TelnetEnabled       (True / False)   [True ]
  SSHEnabled          (True / False)   [False]
  GUIMgmtEnabled      (True / False)   [True ]
  SSLEnabled          (True / False)   [False]
  EmbeddedGUIEnabled  (True / False)   [True ]
  SNMPEnabled         (True / False)   [True ]
  NTPEnabled          (True / False)   [False]
  CIMEnabled          (True / False)   [False]
  FTPEnabled          (True / False)   [True ]
  MgmtServerEnabled   (True / False)   [True ]

  Do you want to save and activate this services setup? (y/n): [n]
```

Set Setup SNMP

Configures SNMP on the switch.

Authority Admin session

Syntax **set setup snmp**

Prompts you in a line-by-line fashion to change SNMP configuration settings. Table 13-22 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table 13-22. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the switch. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Location	Specifies the name of the switch location. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning.
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.

Table 13-22. SNMP Configuration Settings (Continued)

Entry	Description
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “private”.
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

Examples

The following is an example of the Set Setup SNMP command:

```
SANbox (admin) #> set setup snmp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Trap Severity Options
  ---------------------
  unknown, emergency, alert, critical, error, warning, notify, info, debug, mark
  SNMPEnabled         (True / False)               [True             ]
  Contact             (string, max=64 chars)      [<sysContact undefined>]
  Location            (string, max=64 chars)      [<sysLocation undefined>]
  Trap1Address        (dot-notated IP Address)    [10.20.71.15      ]
  Trap1Port           (decimal value)             [162              ]
  Trap1Severity       (see allowed options above) [warning          ]
  Trap1Version        (1 / 2)                     [2                ]
  Trap1Enabled        (True / False)              [False            ]
  Trap2Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap2Port           (decimal value)             [162              ]
  Trap2Severity       (see allowed options above) [warning          ]
  Trap2Version        (1 / 2)                     [2                ]
  Trap2Enabled        (True / False)              [False            ]
  Trap3Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap3Port           (decimal value)             [162              ]
  Trap3Severity       (see allowed options above) [warning          ]
  Trap3Version        (1 / 2)                     [2                ]
  Trap3Enabled        (True / False)              [False            ]
  Trap4Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap4Port           (decimal value)             [162              ]
  Trap4Severity       (see allowed options above) [warning          ]
  Trap4Version        (1 / 2)                     [2                ]
  Trap4Enabled        (True / False)              [False            ]
  Trap5Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap5Port           (decimal value)             [162              ]
  Trap5Severity       (see allowed options above) [warning          ]
  Trap5Version        (1 / 2)                     [2                ]
  Trap5Enabled        (True / False)              [False            ]
  ReadCommunity       (string, max=32 chars)      [public           ]
  WriteCommunity      (string, max=32 chars)      [private          ]
  TrapCommunity       (string, max=32 chars)      [public           ]
  AuthFailureTrap     (True / False)              [False            ]
  ProxyEnabled        (True / False)              [True             ]
```

Set Setup System

Configures the network, session, and logging settings on the switch.

Authority Admin session

Syntax **set setup system**

Prompts you in a line-by-line fashion to change system configuration settings. Table 13-23 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

NOTE: Changing the IP address will terminate all Ethernet management sessions.

Table 13-23. System Configuration Settings

Entry	Description
EthNetworkEnable	Enables (True) or disables (False) the Ethernet port. The default is True.
EthNetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
EthNetworkAddress	Ethernet Internet Protocol (IP) address. The default is 10.0.0.1.
EthNetworkMask	Ethernet subnet mask address. The default is 255.0.0.0.
EthGatewayAddress	Ethernet IP address gateway. The default is 10.0.0.254
AdminTimeout	Amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
InactivityTimeout	Amount of time in minutes the switch waits before terminating an idle Telnet command line interface session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.

Table 13-23. System Configuration Settings (Continued)

Entry	Description
NTPClientEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) client on the switch. This client enables the switch to synchronize its time with an NTP server. This feature supports NTP version 4 and is compatible with version 3. An Ethernet connection to the server is required and you must first set an initial time and date on the switch. The synchronized time becomes effective immediately. The default is False.
NTPServerAddress	The IP address of the NTP server from which the NTP client acquires the time and date. The default is 10.0.0.254.
EmbeddedGUIEnabled	Enables (True) or disables (False) the QuickTools management application. Changing this parameter to False while QuickTools is running will terminate the application. The default is True.

Examples

The following is an example of the Set Setup System command:

```
SANbox (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

EthNetworkDiscovery     (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
EthNetworkAddress       (dot-notated IP Address)             [10.0.0.1     ]
EthNetworkMask          (dot-notated IP Address)             [255.255.255.0]
EthGatewayAddress       (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
InactivityTimeout       (dec value 0-1440 minutes, 0=never)  [0            ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
NTPClientEnabled        (True / False)                       [False        ]
NTPServerAddress        (dot-notated IP Address)             [10.0.0.254   ]
EmbeddedGUIEnabled      (True / False)                       [True         ]
```

Set Switch State

Changes the administrative state for all ports on the switch. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration.

Authority Admin session

Syntax **set switch state [state]**

Keywords **[state]**

[state] can be one of the following:

online

Activates and prepares the ports to send data. This is the default.

offline

Prevents the ports from receiving signal and accepting a device login.

diagnostics

Prepares the ports for testing and prevents each port from accepting a device login. When you leave the diagnostics state, the switch automatically resets.

Examples The following is an example of the Set Switch command:

```
SANbox #>admin start
SANbox (admin) #>set switch state offline
```

Set Timezone

Specifies the time zone for the switch and the workstation. The default is Universal Time (UTC) also known as Greenwich Mean Time (GMT). This keyword prompts you to choose a region, then a subregion to specify the time zone. Changing the time zone converts the current time to the time in the new time zone.

Authority Admin session

Syntax **set timezone**

Examples The following is an example of the Set Timezone command:

```
SANbox (admin) #> set timezone
  Africa                                America
  Antarctica                            Asia
  Atlantic                              Australia
  Europe                                Indian
  Pacific                               UTC
        Press ENTER for more options or 'q' to make a selection.

  America/Grenada                       America/Guadeloupe
  America/Guatemala                     America/Guayaquil
  America/Guyana                        America/Halifax
  America/Havana                        America/Hermosillo
  America/Indiana                       America/Indianapolis
  .
  .
  .
  America/Monterrey                     America/Montevideo
  America/Montreal                      America/Montserrat
  America/Nassau                        America/New_York
  America/Nipigon                       America/Nome
  America/Noronha                       America/North_Dakota
  America/Panama                        America/Pangnirtung

        Press ENTER for more options or 'q' to make a selection.
q
  Enter selection (or 'q' to quit): america/north_dakota
  America/North_Dakota/Center
  Enter selection (or 'q' to quit): america/north_dakota/center
```

Show About

Displays an introductory set of information about operational attributes of the switch. This command is equivalent to the Show Version command.

Authority None

Syntax **show about**

Examples The following is an example of the Show About command:

```
SANbox #> show about
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription     SANbox 5000 FC Switch
       EthNetworkAddress     10.20.11.192 (use 'set setup system' to update)
       EthMACAddress         00:c0:dd:00:71:ee
       WorldWideName         10:00:00:c0:dd:00:71:ed
       ChassisSerialNumber   FAM033100024
       SymbolicName          SANbox
       ActiveSWVersion       V6.7.x.x.xx.xx
       ActiveTimestamp       day month date time year
       DiagnosticsStatus     Passed
          LicensedPorts         20
```

Show Alarm

Displays the alarm log and session output stream display setting.

Authority None

Syntax **show alarm**
settings

Keywords ***settings***

Displays the status of the parameter that controls the display of alarms in the session output stream. This parameter is set using the Set Alarm command.

Notes The alarm log is cleared when the switch is reset or power cycled.

Examples The following is an example of the Show Alarm command:

```
  [1][Fri Jan 19 13:50:26.508 UTC 2007][A][1004.000F][Port: 4][Eport Isolating
due to Merge Zone Failure]
  [2][Fri Jan 19 13:50:26.513 UTC 2007][A][1004.0030][Topology change, lost
route to switch with domain ID 1]
  [3][Sun Jan 21 07:59:28.677 UTC 2007][A][1004.0030][Topology change, lost
route to switch with domain ID 99]
  [4][Sun Jan 21 07:59:29.367 UTC 2007][A][1004.0030][Topology change, lost
route to switch with domain ID 101]
```

The following is an example of the Show Alarm Settings command:

```
SANbox #> show alarm settings

  Current settings for alarm
  --------------------------
  display  ON
```

Show Broadcast

Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

Authority None

Syntax **show broadcast**

Examples The following is an example of the Show Broadcast command:

```
SANbox #> show broadcast

  Group Member Ports ISL Ports
  ----- ------------ ---------
  0     3            16
        15
        16
```

Show Chassis

Displays chassis component status and temperature.

Authority None

Syntax **show chassis**

Examples The following is an example of the Show Chassis command for model 5602.

```
SANbox #> show chassis
   Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   36
  FanStatus (1)                     Good
  FanStatus (2)                     Good
  FanDirection (1)                  BackToFront
  FanDirection (2)                  BackToFront
  PowerSupplyStatus (1)             Good
  PowerSupplyStatus (2)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

Show Config Port

Displays configuration parameters for one or more ports.

Authority None

Syntax **show config port *[port_number]***

Keywords ***[port_number]***

The number of the port. Ports are numbered beginning with 0. If you omit [port_number], all ports are specified.

Examples The following is an example of the Show Config Port command for port 3:

```
SANbox #> show config port 3

  Configuration Name: default
  ---------------------------

  Port Number: 3
  ------------
  AdminState         Offline
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port3
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  LCFEnabled         False
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Disabled
  VIEnabled          False
  MFSEnabled         True
  PDISCPingEnable    True
```

The following is an example of the Show Config Port command for a 10-Gbps port:

```
SANbox #> show config port 16
  Configuration Name: default
  -------------------
  Port Number: 16
  ------------
  AdminState         Online
  LinkSpeed          10Gb/s
  PortType           G
  SymbolicName       10G-16
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  AutoPerfTuning     False
  LCFEnabled         False
  MFSEnabled         False
  MSEnabled          True
  IOStreamGuard      Disabled
  VIEnabled          False
  PDISCPingEnabled   True
```

Show Config Security

Displays the security database configuration parameters.

Authority None

Syntax **show config security**

Examples The following is an example of the Show Config Security command:

```
SANbox #> show config security

  Configuration Name: default
  -------------------

  Switch Security Configuration Information
  -----------------------------------------
  FabricBindingEnabled  False
  AutoSave              True

  Port  Binding Status  WWN
  ----  --------------  ---
  0     Enabled         10:00:00:00:00:00:00:01
  2     Disabled        10:00:00:00:00:00:00:01
  5     Enabled         10:00:00:00:00:00:00:01
                        10:00:00:00:00:00:00:02
```

Show Config Security Portbinding

Displays the port binding configuration for one or more ports.

Authority None

Syntax **show config security portbinding *[port_number]***

Keywords ***[port_number]***

The number of the port. If you omit [port_number], the port binding configuration for all ports is displayed.

Examples The following is an example of the Show Config Security Port command:

```
SANbox #> show config security portbinding

  Configuration Name: default
  -------------------

  Port    Binding Status   WWN
  ----    --------------   -----------------------
  0       Enabled          10:20:30:40:50:60:70:80
  1       Enabled          10:20:30:40:50:60:70:80
  2       Disabled         10:20:30:40:50:60:70:80
  3       Enabled          10:20:30:40:50:60:70:80
  4       Enabled          10:20:30:40:50:60:70:80
  5       Disabled         10:20:30:40:50:60:70:80
  6       Enabled          10:20:30:40:50:60:70:81
  7       Disabled         10:20:30:40:50:60:70:82
  8       Enabled          10:20:30:40:50:60:70:80
```

Show Config Switch

Displays the switch configuration parameters.

Authority None

Syntax **show config switch**

Examples The following is an example of the Show Config Switch command:

```
SANbox #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DefaultDomainID       19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

Show Config Threshold

Displays alarm threshold parameters for the switch.

Authority None

Syntax **show config threshold**

Examples The following is an example of the Show Config Threshold command:

```
SANbox #> show config threshold
  Configuration Name: default
  ------------
  Threshold Configuration Information
  -----------------------------------
  ThresholdMonitoringEnabled      False
  CRCErrorsMonitoringEnabled      True
    RisingTrigger                 25
    FallingTrigger                1
    SampleWindow                  10
  DecodeErrorsMonitoringEnabled   True
    RisingTrigger                 25
    FallingTrigger                0
    SampleWindow                  10
  ISLMonitoringEnabled            True
    RisingTrigger                 2
    FallingTrigger                0
    SampleWindow                  10
  LoginMonitoringEnabled          True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LogoutMonitoringEnabled         True
    RisingTrigger                 5
    FallingTrigger                1
    SampleWindow                  10
  LOSMonitoringEnabled            True
    RisingTrigger                 100
    FallingTrigger                5
    SampleWindow                  10
```

Show Config Zoning

Displays zoning configuration parameters for the switch.

Authority None

Syntax **show config zoning**

Examples The following is an example of the Show Config Zoning command:

```
SANbox #> show config zoning

 Configuration Name: default
  -------------------

  Zoning Configuration Information
  --------------------------------
  InteropAutoSave       True
  DefaultZone           True
  DiscardInactive       False
```

Show Domains

Displays list of each domain and its worldwide name in the fabric.

Authority None

Syntax **show domains**

Examples The following is an example of the Show Domains command:

```
SANbox #> show domains
  Principal switch is (remote): 10:00:00:60:69:50:0b:6c
  Upstream Principal ISL is   : 1
  Domain ID List:
        Domain 97  (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
        Domain 98  (0x62)  WWN = 10:00:00:60:df:22:2e:0c
        Domain 99  (0x63)  WWN = 10:00:00:c0:dd:00:72:45
        Domain 100 (0x64)  WWN = 10:00:00:c0:dd:00:ba:68
        Domain 101 (0x65)  WWN = 10:00:00:60:df:22:2e:06
        Domain 102 (0x66)  WWN = 10:00:00:c0:dd:00:90:ef
        Domain 103 (0x67)  WWN = 10:00:00:60:69:50:0b:6c
        Domain 104 (0x68)  WWN = 10:00:00:c0:dd:00:b8:b7
```

Show Donor

Displays list of current donor and extended credit configuration for all ports.

Authority None

Syntax **show donor**

Examples The following is an example of the Show Donor command:

```
SANbox #> show donor

  Port    Config Ext Credit Max Credit Donated Member of   Valid Groups to
  Number  Type   Requested  Available  to Port Donor Group Extend Credit
  ------  ------ ---------- ---------- ------- ----------- ---------------
  0       GL     0          16         None    0           0
  1       GL     0          16         None    0           0
  2       GL     0          16         None    0           0
  3       GL     0          16         None    0           0
  4       GL     0          16         None    0           0
  5       GL     0          16         None    0           0
  6       GL     0          16         None    0           0
  7       GL     0          16         None    0           0
  8       GL     0          16         None    0           0
  9       GL     0          16         None    0           0
  10      GL     0          16         None    0           0
  11      GL     0          16         None    0           0
  12      GL     0          16         None    0           0
  13      GL     0          16         None    0           0
  14      GL     0          16         None    0           0
  15      GL     0          16         None    0           0
  16      G      0          16         None    None        None
  Donor Group  Credit Pool
  -----------  -----------
  0            0
```

Show Fabric

Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

Authority None

Syntax **show fabric**

Examples The following is an example of the Show Fabric command:

```
SANbox #> show fabric
 Domain     WWN                     Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                     ------------    ----------      ------------
 16 (0x10)  10:00:00:c0:dd:00:77:81 10.20.68.11     0.0.0.0         gui sb1 .11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d 10.20.68.12     0.0.0.0         sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 10.20.68.160    0.0.0.0         sw .160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 10.20.68.108    0.0.0.0         Sb2 .108
```

Show FDMI

Displays detailed information about the device host bus adapter.

Authority None

Syntax **show fdmi *[port_wwn]***

Keywords ***[port_wwn]***

The device world wide port name for which to display information. If you omit [port_wwn], the command displays a summary of host bus adapter information for all attached devices in the fabric. Illegal characters in the display appear as question marks (?).

Examples The following is an example of the Show FDMI command:

```
SANbox #> show fdmi
HBA ID                  PortID  Manufacturer           Model    Ports
--------                ------  ---------------       -------   -----
21:01:00:e0:8b:27:aa:bc 610000  QLogic Corporation    QLA2342   2
21:00:00:00:ca:25:9b:96 180100  QLogic Corporation    QL2330    2
```

The following is an example of the Show FDMI WWN command:

```
SANbox #> show fdmi 21:00:00:e0:8b:09:3b:17
  FDMI Information
  ----------------
  Manufacturer            QLogic Corporation
  SerialNumber            [04202
  Model                   QLA2342
  ModelDescription        QLogic QLA2342 PCI Fibre Channel Adapter
  PortID                  610000
  NodeWWN                 20:00:00:e0:8b:07:aa:bc
  HardwareVersion         FC5010409-10
  DriverVersion           8.2.3.10 Beta 2 (W2K VI)
  OptionRomVersion        1.21
  FirmwareVersion         03.02.13.
  OperatingSystem         SunOS 5.8
  MaximumCTPayload        2040
  NumberOfPorts           1

  Port  21:01:00:e0:8b:27:aa:bc

  SupportedFC4Types       FCP
  SupportedSpeed          2Gb/s
  CurrentSpeed            2Gb/s
  MaximumFrameSize        2048
  OSDeviceName
  HostName
```

Show Interface

Displays the status of the active network interfaces.

Authority None

Syntax **show interface**

Examples The following is an example of the Show Interface command:

```
SANbox #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:BD:ED
          inet addr:10.20.68.107  Bcast:10.20.68.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

Show Log

Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax **show log**
[number_of_events]
component
display [filter]
level
options
port
settings

Keywords **[number_of_events]**

Specifies the number of the most recent events to display from the event log. [number_of_events] must be a positive integer.

component

Displays the components currently being monitored for events. Table 13-24 describes the log monitoring components.

Table 13-24. Log Monitoring Components

Component	Description
Chassis	Chassis hardware components such as fans and power supplies
CLI	Command line interface events
Eport	E_Port events
Mgmtserver	Management server events
Nameserver	Name server events
Other	Miscellaneous events
Port	Port events
SNMP	SNMP events
Switch	Switch management events
Zoning	Zoning conflict events

display [filter]

Displays log events on the screen according to the component or severity level filter given by [filter]. [filter] can be one of the following:

Info

Displays all informative events.

Warning

Displays all warning events.

Critical

Displays all critical events.

Eport3

Displays all events related to E_Ports.

Mgmtserver

Displays all events related to the management server.

Nameserver

Displays all events related to the name server.

Port [port_number]

Displays all events related to the port given by [port_number].

SNMP

Displays all events related to SNMP.

Switch

Displays all events related to switch management.

Zoning

Displays all events related to zoning.

level

Displays the event severity level logging setting and the display level setting.

options

Displays the options that are available for configuring event logging and automatic display to the screen. Refer to the "Set Log" command on page 13-76 for information about how to configure event logging and display level.

port

Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings

Displays the current filter settings for component, severity level, port, and display level. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples

The following is an example of the Show Log Component command:

```
SANbox #> show log component
Current settings for log
   ------------------------
   FilterComponent   NameServer MgmtServer Zoning Switch Blade Port Eport Snmp
```

The following is an example of the Show Log Level command:

```
SANbox #> show log level
   Current settings for log
   ------------------------
   FilterLevel       Info
   DisplayLevel      Critical
```

The following is an example of the Show Log Options command:

```
SANbox #> show log options
  Allowed options for log
  -----------------------
   FilterComponent   All,None,NameServer,MgmtServer,Zoning,Switch,Blade,Port,Eport,Snmp,CLI
   FilterLevel       Critical,Warn,Info,None
   DisplayLevel      Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
SANbox #> show log
   [327][day month date time year][I][Eport Port:0/8][Eport State=
   E_A0_GET_DOMAIN_ID]
   [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
   [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
   [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
   [331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
   [332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
   len= 0x30]
   [333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
   [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
   [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
```

Show LSDB

Displays Link State database information,

Authority None

Syntax **show lsdb**

Examples The following is an example of the Show LSDB command:

```
SANbox #> show lsdb

  Link State Database Information
  -------------------------------
  LsID 34:  Age=1176, Incarnation=0x800000e5
    NeighborDomain=36, LocalPort=6, RemotePort=7, Cost=500
    NeighborDomain=35, LocalPort=16, RemotePort=16, Cost=100
    NeighborDomain=35, LocalPort=18, RemotePort=19, Cost=100
    NeighborDomain=35, LocalPort=7, RemotePort=7, Cost=500
    NeighborDomain=35, LocalPort=5, RemotePort=4, Cost=500

    Local Domain

  LsID 35:  Age=1166, Incarnation=0x800000cc
    NeighborDomain=34, LocalPort=16, RemotePort=16, Cost=100
    NeighborDomain=34, LocalPort=19, RemotePort=18, Cost=100
    NeighborDomain=36, LocalPort=5, RemotePort=4, Cost=250
    NeighborDomain=34, LocalPort=7, RemotePort=7, Cost=500
    NeighborDomain=34, LocalPort=4, RemotePort=5, Cost=500

    Route: OutPort=18, Hops=1, Cost=100

  LsID 36:  Age=1162, Incarnation=0x80000046
    NeighborDomain=34, LocalPort=7, RemotePort=6, Cost=500
    NeighborDomain=35, LocalPort=4, RemotePort=5, Cost=250

    Route: OutPort=16, Hops=2, Cost=350
```

Show Media

NOTE: This command requires the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider or authorized reseller.

Displays transceiver operational and diagnostic information for one or more ports.

Authority

None

Syntax

show media
[port_list]
all
installed

Keywords

[port_list]

The port or ports for which to display transceiver information. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15.

all

Displays transceiver information for all ports.

installed

Displays transceiver information for all ports that have transceivers installed.

Notes

Table 13-25 describes the transceiver information in the Show Media display.

Table 13-25. Transceiver Information

Information Type	Description
MediaType	Fibre Channel specification or one of the following: ■ NotInstalled–transceiver is not installed. ■ Unknown–transceiver does not have a serial ID. ■ NotApplicable–transceiver is not needed.
MediaVendor	Vendor name
MediaPartNumber	Vendor media part number
MediaRevision	Vender media revision level
MediaSerialNumber	Vendor media serial number
MediaSpeeds	Transmission speed capabilities

Table 13-25. Transceiver Information (Continued)

Information Type	Description
Temp	Temperature in degrees Celsius.
Voltage	Supply voltage in Volts. The range is 0–6.55.
Tx Bias	Transmitter laster bias current in milliamps. The range is 0–655.
Tx Power	Transmitter coupled output power in milliWatts. The range is 0–6.55.
Rx Power	Received optical power in milliWatts. The range is 0–6.55.
Value	Measured value.
Status	State associated with the measured value: ■ Normal: Value is in the normal operating range. ■ HighAlarm: Value exceeds the high alarm threshold. ■ HighWarning: Value exceeds the high warning threshold. ■ LowWarning: Value is less than the low warning threshold. ■ LowAlarm: Value is less than the low alarm threshold.
HighAlarm	Vendor specified threshold above which an alarm is issued.
HighWarning	Vendor specified threshold above which a warning is issued.
LowWarning	Vendor specified threshold below which a warning is issued.
LowAlarm	Vendor specified threshold below which an alarm is issued.

Examples

The following is an example of the Show Media command for port 4:

```
SANbox #> show media 4
Port Number: 4
-------------
MediaType           400-M5-SN-I
MediaVendor         FINISAR CORP.
MediaPartNumber     FTRJ8524P2BNL
MediaRevision       A
MediaSerialNumber   P6G22RL
MediaSpeeds         1Gb/s, 2Gb/s, 4Gb/s

                       Temp     Voltage      Tx Bias      Tx Pwr      Rx Pwr
                        (C)         (V)         (mA)        (mW)        (mW)
                  ---------- ---------- ------------ ---------- ----------
       Value          37.32        3.33         7.30       0.373       0.000
       Status        Normal HighWarning       Normal      Normal    LowAlarm
       HighAlarm      95.00        3.90        17.00       0.637       1.264
       HighWarning    90.00        3.70        14.00       0.637       0.791
       LowWarning    -20.00        2.90         2.00       0.082       0.028
       LowAlarm      -25.00        2.70         1.00       0.073       0.019
```

The following is an example of the Show Media command for all ports:

```
SANbox #> show media
Note: -- LowAlarm; - LowWarning; + HighWarning; ++ HighAlarm
Port Vendor Name     Temp    Voltage Tx Bias Tx Pwr Rx Pwr
Num                  (C)     (V)     (mA)    (mW)   (mW)
---- -----------     ------- ------- ------- ------ ------
0    NotInstalled     N/A     N/A     N/A     N/A    N/A
1    NotApplicable    N/A     N/A     N/A     N/A    N/A
2    Unknown          N/A     N/A     N/A     N/A    N/A
3    FINISAR          N/A     N/A     N/A     N/A    N/A
4    FINISAR         37.32   3.33+   7.30    0.371  0.000 --
5    FINISAR         37.32   3.33+   7.30    0.371  0.000 --
6    FINISAR         37.32   3.33+   7.30    0.371  0.000 --
7    FINISAR         37.32   3.33+   7.30    0.371  0.000 --
8    FINISAR         37.32   3.33+   7.30    0.371  0.000 --
9    FINISAR         37.32   3.33+   7.30    0.371  0.000 --
10   FINISAR         37.32   3.33+   7.30    0.371  0.000 --
11   FINISAR         37.32   3.33+   7.30    0.371  0.000 --
12   FINISAR         37.32   3.33+   7.30    0.371  0.000 --
13   FINISAR         37.32   3.33+   7.30    0.371  0.000 --
14   FINISAR         37.32   3.33+   7.30    0.371  0.000 --
15   FINISAR         37.32   3.33+   7.30    0.371  0.000 --
16   Unknown          N/A     N/A     N/A     N/A    N/A
17   INFINEON         N/A     N/A     N/A     N/A    N/A
18   INFINEON        39.62    N/A    5.84    0.637  0.092
19   INFINEON        39.62    N/A    5.84    0.637  0.092
```

Show Mem

Displays information about memory activity.

Authority None

Syntax **show mem *[count]***

Keywords ***[count]***

The number of seconds for which to display memory information. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

NOTE: This keyword will display memory activity updates until [count] is reached–it cannot be interrupted. Therefore, avoid using large values for [count].

Examples The following is an example of the Show Mem command:

```
SANbox #> show mem

   procs                      memory    swap          io     system         cpu
 r  b  w   swpd   free   buff  cache  si  so    bi    bo   in    cs  us  sy  id
 0  0  0      0 144924    884  60104   0   0     0     0  119    73   1   2  97

Filesystem space in use: 36156/40155 KB (90%)
```

Show NS

Displays the WWNs for devices in the fabric.

Authority None

Syntax **show ns *[option]***

Keywords ***[option]***

The domain IDs or port IDs for which to display name server information. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all

Displays WWNs for all switches and ports.

[domain_id]

Displays WWNs for all devices connected to the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]

Displays the WWNs for the devices connected to the port given by [port_id]. [port_id] is a port Fibre Channel address.

Examples The following is an example of the Show NS (local domain) command:

```
SANbox #> show ns
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   19 (0x13) 1301e1 NL   3   21:00:00:20:37:73:13:69 20:00:00:20:37:73:13:69
  2   19 (0x13) 1301e2 NL   3   21:00:00:20:37:73:12:9b 20:00:00:20:37:73:12:9b
  3   19 (0x13) 1301e4 NL   3   21:00:00:20:37:73:05:26 20:00:00:20:37:73:05:26
  4   19 (0x13) 130d00 N    3   21:01:00:e0:8b:27:a7:bc 20:01:00:e0:8b:27:a7:bc
```

The following is an example of the Show NS [domain_ID] command:

```
SANbox #> show ns 18
    Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   18 (0x12) 120700 N    3   21:00:00:e0:8b:07:a7:bc 20:00:00:e0:8b:07:a7:bc
```

The following is an example of the Show NS [port_ID] command:

```
SANbox #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName
  NodeIPAddress     0.0.0.0
  ClassOfService    3
  PortIPAddress     0.0.0.0
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

Show Pagebreak

Displays the current pagebreak setting.

Authority None

Syntax **show pagebreak**

Notes The pagebreak setting limits the display of information to 20 lines or allows the continuous display of information without a break.

Examples The following is an example of the Show Pagebreak command:

```
SANbox #> show pagebreak

  current setting: ON
```

Show Perf

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second. Transmission rates are expressed in thousands (K) and millions (M).

Authority None

Syntax

show perf *[port_list]*

or

show perf

byte *[port_list]*
inbyte *[port_list]*
outbyte *[port_list]*
frame *[port_list]*
inframe *[port_list]*
outframe *[port_list]*
errors *[port_list]*

Keywords ***[port_list]***

Displays the instantaneous performance data for up to sixteen ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for all ports.

byte *[port_list]*

Displays continuous performance data in total bytes/second transmitted and received for up to sixteen ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

inbyte *[port_list]*

Displays continuous performance data in bytes/second received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

outbyte *[port_list]*

Displays continuous performance data in bytes/second transmitted for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

frame *[port_list]*

Displays continuous performance data in total frames/second transmitted and received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

inframe *[port_list]*

Displays continuous performance data in frames/second received for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

outframe *[port_list]*

Displays continuous performance data in frames/second transmitted for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

errors *[port_list]*

Displays continuous error counts for the ports given by [port_list]. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15. If you omit [port_list], the command displays performance data for ports 0–15. Type “q” and press the Enter key to stop the display.

Examples

The following is an example of the Show Perf command:

```
SANbox #> show perf
  Port   Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
  Number   (in)       (out)    (total)      (in)       (out)    (total)
  ------ -------    -------    -------    --------   --------   --------
  0      7K         136M       136M       245        68K        68K
  1      58K        0          58K        1K         0          1K
  2      0          0          0          0          0          0
  3      0          0          0          0          0          0
  4      0          0          0          0          0          0
  5      0          0          0          0          0          0
  6      0          7K         7K         0          245        245
  7      136M       58K        136M       68K        1K         70K
  8      7K         136M       136M       245        68K        68K
  9      58K        0          58K        1K         0          1K
  10     0          0          0          0          0          0
  11     0          0          0          0          0          0
  12     0          0          0          0          0          0
  13     0          0          0          0          0          0
  14     0          7K         7K         0          245        245
  15     136M       58K        136M       68K        1K         70K
  16     47M        23K        47M        23K        726        24K
  17     0          0          0          0          0          0
  18     23K        47M        47M        726        23K        24K
  19     0          0          0          0          0          0
```

The following is an example of the Show Perf Byte command:

```
SANbox #> show perf byte
Displaying bytes/sec (total)...  (Press any key to stop display)

  0    1    2    3    4    5    6    7    8    9    10   11   12   13   14   15
  ---------------------------------------------------------------------------
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    135M 58K  0    0    0    0    7K   135M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
q
```

Show Port

Displays operational information for one or more ports.

Authority None

Syntax **show port**
[port_list]

Keywords **[port_list]**
The number of the port for which to display information. [port_list] can be a set of port numbers and ranges delimited by spaces. For example, [0 2 10-15] specifies ports 0, 2, 10, 11, 12, 13, 14, and 15.

Notes Table 13-26 describes the port parameters.

Table 13-26. Show Port Parameters

Entry	Description
AdminState	Administrative state
AIinit	Incremented each time the port begins AL initialization.
AIinitError	Number of times the port entered initialization and the initialization failed.
AsicNumber	ASIC number
AsicPort	ASIC port number
Bad Frames	Number of frames that have framing errors.
BBCR_FrameFailures	Number of times more frames were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
BBCR_RRDYFailures	Number of times more R_RDYs were lost during a credit recovery period than the recovery process could resolve. This causes a Link Reset to recover the credits.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
ConfigType	Configured port type

Table 13-26. Show Port Parameters (Continued)

Entry	Description
DecodeError	Number of decode errors detected
DiagFaultCode	Fault code from the most recent Power-on self test
DiagStatus	Status from the most recent Power-on self test
EpConnects	Number of times an E_Port connected through ISL negotiation.
EpConnState	E_Port connection status
EpIsoReason	E_Port isolation reason
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Number of frames received there were no available credits.
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
IOStreamGuard	I/O StreamGuard status
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
LinkSpeed	Port transmission speed
LinkState	Port activity status
LIP_AL_PD_ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP_F7_AL_PS	This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.

Table 13-26. Show Port Parameters (Continued)

Entry	Description
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Login	Number of device logins
LoginStatus	Login status
Logout	Number of device logouts
LongFramesIn	Number of incidents when one or more frames are received that are greater than the maximum size.
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
LostFrames	Number of incidents of lost frames.
Lost RRDYs	Number of incidents of lost R_RDYs.
MaxCredit	Maximum number of port buffer credits
MediaSpeeds	Possible transmission speeds
MediaPartNumber	Transceiver vendor part number
MediaRevision	Transceiver revision
MediaType	Transceiver type
MediaVendor	Transceiver manufacturer
MediaVendorID	Transceiver manufacturer identifier
OperationalState	Operational state
PerfTuningMode	AutoPerfTuning status
PortID	Fibre Channel port address
PortWWN	World wide port name
PrimSeqErrors	Primitive sequence errors detected.
RunningType	Operational port type
RxLinkResets	Number of link reset primitives received from an attached device.

Table 13-26. Show Port Parameters (Continued)

Entry	Description
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
ShortFramesIn	Number of incidents when one or more frames are received that are less than the minimum size.
SymbolicName	Port symbolic name
SyncStatus	Synchronization status
TestFaultCode	Fault code from the most recent port test
TestStatus	Status from the most recent port test
TotalErrors	Total number of errors detected.
TotalLinkResets	Total number of link resets.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Number of Offline Sequences issued by this port.
XmitterEnabled	Transmitter status

Examples

The following is an example of the Show Port command:

```
SANbox #> show port 1
  Port Number: 1
  ------------
  AdminState       Online              OperationalState Offline
  AsicNumber       0                   PerfTuningMode   Normal
  AsicPort         0                   PortID           220000
  ConfigType       GL                  PortWWN          20:00:00:c0:dd:07:20:58
  DiagStatus       Passed              RunningType      Unknown
  EpConnState      None                MediaPartNumber  PL-XPL-VC-SG3-22
  EpIsoReason      NotApplicable       MediaRevision    1
  IOStreamGuard    Disabled            MediaType        400-M5-SN-I
  LinkSpeed        Auto                MediaVendor      PICOLIGHT
  LinkState        Inactive            MediaVendorID    00000485
  LoginStatus      NotLoggedIn         SymbolicName     Port0
  MaxCredit        16                  SyncStatus       SyncLost
  MediaSpeeds      1Gb/s, 2Gb/s, 4Gb/s XmitterEnabled   True

  ALInit             2                   LIP_F8_F7          0
  ALInitError        0                   LinkFailures       0
  BadFrames          0                   Login              0
  BBCR_FrameFailures 0                   Logout             0
  BBCR_RRDYFailures  0                   LongFramesIn       0
  Class2FramesIn     0                   LoopTimeouts       0
  Class2FramesOut    0                   LossOfSync         0
  Class2WordsIn      0                   LostFrames         0
  Class2WordsOut     0                   LostRRDYs          0
  Class3FramesIn     0                   PrimSeqErrors      0
  Class3FramesOut    0                   RxLinkResets       0
  Class3Toss         0                   RxOfflineSeq       0
  Class3WordsIn      0                   ShortFramesIn      0
  Class3WordsOut     0                   TotalErrors        0
  DecodeErrors       0                   TotalLinkResets    0
  EpConnects         0                   TotalLIPsRecvd     0
  FBusy              0                   TotalLIPsXmitd     4
  FlowErrors         0                   TotalOfflineSeq    3
  FReject            0                   TotalRxFrames      0
  InvalidCRC         0                   TotalRxWords       0
  InvalidDestAddr    0                   TotalTxFrames      0
  LIP_AL_PD_AL_PS    0                   TotalTxWords       0
  LIP_F7_AL_PS       0                   TxLinkResets       0
  LIP_F7_F7          0                   TxOfflineSeq       3
  LIP_F8_AL_PS       0
```

Show Post Log

Displays the Power On Self Test (POST) log which contains results from the most recently failed POST.

Authority None

Syntax **show post log**

Examples The following is an example of the Show Post Log command:

```
SANbox #> show post log

  Sat Jan  1 00:18:21 2000: POST log created
  Sat Jan  1 00:18:34 2000: POST completed
```

Show Setup Mfg

Displays manufacturing information about the switch.

Authority None

Syntax **show setup mfg**

Examples The following is an example of the Show Setup Mfg command for a model 5600 switch:

```
SANbox #> show setup mfg
  Manufacturing Information
  -------------------------
  BrandName               QLogic
  BuildDate               Unknown
  PartNumber              SANbox 5600
  SerialNumber            FAM0331000011
  LicensedPorts           20
  MACAddress              00:c0:dd:02:cc:17
  PlanarPartNumber        Unknown
  SwitchSymbolicName      SANbox
  SwitchWWN               10:00:00:c0:dd:02:cc:16
  SystemDescription       SANbox 5600 FC Switch
  SystemObjectID          1.3.6.1.4.1.1663.1.1.1.1.23
```

Show Setup Radius

Displays RADIUS server information.

Authority None

Syntax **show setup radius**

Examples The following is an example of the Show Setup RADIUS command:

```
SANbox #> show setup radius

  Radius Information
  ------------------
  DeviceAuthOrder   RadiusLocal
  UserAuthOrder     RadiusLocal
  TotalServers      1

  Server: 1

  ServerIPAddress   10.20.11.8
  ServerUDPPort     1812
  DeviceAuthServer  False
  UserAuthServer    True
  AccountingServer  False
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********
```

Show Setup Services

Displays switch service status information.

Authority None

Syntax **show setup services**

Examples The following is an example of the Show Setup Services command:

```
SANbox #> show setup services
System Services
----------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLEnabled                False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
MgmtServerEnabled         True
```

Show Setup SNMP

Displays the current SNMP settings.

Authority None

Syntax **show setup snmp**

The following is an example of the Show Setup Snmp command:

```
SANbox #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           SANbox 5000 FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
  ObjectID              1.3.6.1.4.1.1663.1.1.1.1.17
  AuthFailureTrap       True
  ProxyEnabled          True
```

Show Setup System

Displays the current system settings.

Authority None

Syntax **show setup system**

Examples The following is an example of the Show Setup System command:

```
SANbox #> show setup system
  System Information
  ------------------
  EthNetworkEnable         True
  EthNetworkDiscovery      Static
  EthNetworkAddress        10.20.11.32
  EthNetworkMask           255.255.252.0
  EthGatewayAddress        10.20.8.254
  AdminTimeout             30
  InactivityTimeout        0
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
  NTPClientEnabled         True
  NTPServerAddress         51.68.85.102
  EmbeddedGUIEnabled       True
```

Show Steering

Displays the routes that data takes in the fabric.

Authority None

Syntax **show steering *[domain_id]***

Keywords ***[domain_id]***

The domain ID for which to display route information. If you omit [domain_id], the system displays routes for all switches in the fabric.

Examples The following is an example of the Show Steering command:

```
SANbox #> show steering 35

  DomainID    DefaultOutPort    InPort OutPort
  --------    --------------    ------ -------
  35          18                3      16/18/16/18
                                5      18/16/18/16
                                6      16/18/16/18
                                7      16/18/16/18
                                15     18/16/18/16
```

Show Switch

Displays switch operational information.

Authority None

Syntax **show switch**

Notes Table 13-27 describes the switch operational parameters.

Table 13-27. Switch Operational Parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch world wide name
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	FC address of switch port 0
FlashSize - MBytes	Size of the flash memory in megabytes
LogFilterLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch
NumberOfSwitchResets	Number of times the switch has been reset over its service life
ReasonForLastReset	Action that caused the last reset
ActiveImageVersion - build date	Active firmware image version and build date.
PendingImageVersion - build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle.
ActiveConfiguration	Name of the switch configuration that is in use.
AdminState	Switch administrative state
AdminModeActive	Admin session status
Beacon	Beacon status as set by the Set Beacon command.
OperationalState	Switch operational state

Table 13-27. Switch Operational Parameters (Continued)

Parameter	Description
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
BoardTemp (1) - Degrees Celsius	Internal switch temperature at circuit board sensor 1.
SwitchDiagnosticsStatus	Results of the power-on self test
SwitchTemperatureStatus	Switch temperature status: normal, warning, failure.

Examples

The following is an example of the Show Switch command:

```
SANbox #> show switch
 Switch Information
 ------------------
 SymbolicName                    SANbox
 SwitchWWN                       10:00:00:c0:dd:00:bc:56
 BootVersion                     Vx.x.x.x-0 (day month date time year)
 CreditPool                      0
 DomainID                        19 (0x13)
 FirstPortAddress                130000
 FlashSize - MBytes              128
 LogFilterLevel                  Critical
 MaxPorts                        20
 NumberOfSwitchResets            15
 ReasonForLastReset              PowerUp
 ActiveImageVersion - build date Vx.x.x.0 (day month date time year)
 PendingImageVersion - build date Vx.x.x.0 (day month date time year)
 ActiveConfiguration             default
 AdminState                      Online
 AdminModeActive                 False
 Beacon                          Off
 OperationalState                Online
 PrincipalSwitchRole             False
 BoardTemp (1) - Degrees Celsius 32
 SwitchDiagnosticsStatus         Passed
 SwitchTemperatureStatus         Normal
```

Show Timezone

Displays the current time zone setting.

Authority None

Syntax **show timezone**

Examples The following is an example of the Show Timezone command:

```
SANbox #> show timezone

  America/Chicago
```

Show Topology

Displays all connected devices.

Authority None

Syntax **show topology**

Examples The following is an example of the Show Topology command:

```
SANbox #> show topology
Unique ID Key
-------------
A = ALPA,  D = Domain ID,  P = Port ID
Port   Local Local                    Remote  Remote                    Unique
Number Type  PortWWN                  Type    NodeWWN                   ID
------ ----- -------                  ------  -------                   ------
5      F     20:05:00:c0:dd:00:bd:ec   N      20:00:00:00:c9:22:1e:93   010500 P
10     E     20:0a:00:c0:dd:00:bd:ec   E      10:00:00:c0:dd:00:80:21   4(0x4) D
```

The following is an example of the Show Topology command for port 1:

```
SANbox  #> show topology 1
  Local Link Information
  ----------------------
  PortNumber 1
  PortID     650100
  PortWWN    20:01:00:c0:dd:00:91:11
  PortType   F

Remote Link Information
-----------------------
Device 0
NodeWWN 50:80:02:00:00:06:d5:38
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 1
NodeWWN 20:00:00:20:37:2b:08:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 2
Description (NULL)
IPAddress 0.0.0.0

Device 3
NodeWWN 20:00:00:20:37:2b:05:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0
```

Show Users

Displays a list of logged-in users. This is equivalent to the User List command.

Authority None

Syntax **show users**

Examples The following is an example of the Show Users command:

```
SANbox #> show users
  User                        Ethernet Addr-Port    Logged in Since
  ----                        ------------------    ---------------
  cim@OB-session1             cim                   Tue Jul 11 05:14:54 2006
  admin@OB-session2           10.20.34.42-3720      Tue Jul 11 12:26:20 2006
  admin@OB-session3           10.20.32.58-35794     Tue Jul 11 11:08:18 2006
  snmp@IB-session4            Unknown               Tue Jul 11 05:15:01 2006
  snmp@OB-session5            Unknown               Tue Jul 11 05:15:01 2006
  admin@OB-session8           10.20.33.201          Tue Jul 11 09:55:36 2006
  admin@OB-session11          10.20.34.42           Tue Jul 11 12:18:20 2006
  admin@OB-session14          10.20.32.68           Tue Jul 11 13:00:40 2006
  ms@OB-session16             Unknown               Tue Jul 11 13:08:31 2006
```

Show Version

Displays an introductory set of information about operational attributes of the switch. This command is equivalent to the Show About command.

Authority None

Syntax **show version**

Examples The following is an example of the Show Version command.

```
SANbox #> show version
       **************************************************
       *                                                *
       *       Command Line Interface SHell  (CLISH)    *
       *                                                *
       **************************************************

       SystemDescription     SANbox 5000 FC Switch
       EthNetworkAddress     10.20.11.192 (use 'set setup system' to update)
       EthMACAddress         00:c0:dd:00:71:ee
       WorldWideName         10:00:00:c0:dd:00:71:ed
       ChassisSerialNumber   FAM033100024
       SymbolicName          SANbox
       ActiveSWVersion       V6.7.x.x.xx.xx
       ActiveTimestamp       day month date time year
       DiagnosticsStatus     Passed
       LicensedPorts         20
```

Shutdown

Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin session

Syntax **shutdown**

Notes When the shutdown is complete, the Heartbeat LED is extinguished.

Test Cancel

Cancels a port test that is in progress.

Authority Admin session

Syntax **test cancel**
port [port_number]

Keywords **port [port_number]**
Cancel the test for the port given by [port_number]. [port_number] can be 0–19.

Examples The following example cancels the test running on port 15:

```
SANbox (admin) #> test cancel port 15
```

Test Port

Tests individual ports using an offline or online test.

Authority Admin session

Syntax **test port [port_number]**
offline [loopback_type]
online

Keywords **[port_number]**

The port to be tested. [port_number] can be 0–19.

offline [loopback_type]

Performs an offline test of the type given by [loopback_type] on the port given by [port_number]. Use the Set Port command to place the port in the diagnostics state before running the test. [loopback_type] can have the following values:

internal

Exercises the internal port connections.

NOTE: An internal test on a 10-Gbps port verifies that a complete path exists, but does not send a test frame.

external

Exercises the port and its transceiver. A transceiver with a loopback plug is required for the port.

NOTE: An external test on a 10-Gbps port verifies that a complete path exists, but does not send a test frame.

online

Exercises the port, transceiver, and device connections while the port is online. This test does not disrupt communication on the port.

Notes

Table 13-28 describes the port test parameters.

Table 13-28. Port Test Parameters

Parameter	Description
LoopCount	Number of frames sent
FrameSize	Number of bytes in each test frame
DataPattern	Pattern in the payload
StopOnError	Stops the test when an error occurs (True). Otherwise, the test continues to completion.
LoopForever	Restarts the test after completion and continues until you cancel it (True). Otherwise, the test ends normally after completion.

To cancel a port test that is in progress, enter the Test Cancel Port command.

To display the status of the most recent port test or port test in progress, enter the Test Status Port command.

Examples

The following example performs an online test on port 1:

```
SANbox #> admin start
SANbox (admin) #> test port 1 online

A list of attributes with formatting and current values will follow. Enter a new
value or simply press the ENTER key to accept the default value. If you wish to
terminate this process before reaching the end of the list press 'q' or 'Q' and the
ENTER key to do so.

LoopCount     (decimal value, 1-4294967295)   [429496729]
FrameSize     (decimal value, 40-2148)        [256      ]
DataPattern   (32-bit hex value or 'Default') [Default  ]
StopOnError   (True / False)                  [True     ]
LoopForever   (True / False)                  [False    ]

Do you want to start the test? (y/n) [n] y

The test has been started.
A notification with the test result(s) will appear
on the screen when the test has completed.

SANbox (admin) #>
  Test for port 1 Passed.
```

Test Status

Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Authority None

Syntax **test status**

port [port_number]

Keywords **port [port_number]**

Display test status for the port given by [port_number]. [port_number] can be 0–19.

Examples The following is an example of the Test Status Port command:

```
SANbox (admin) #> test status port 1
Port               Test                Test               Loop      Test
Num      Port      Type                Status            Count  Failures
----     --------  ----                ------            -----  --------
1        1         Offline Internal    Passed               12         0
```

Uptime

Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax **uptime**

Examples The following is an example of the Uptime command:

```
SANbox #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User

Administers and displays user accounts.

Authority Admin account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax

user
accounts
add
delete [account_name]
edit
list

Keywords

accounts

Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add

Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 8–20 characters.
- Admin authority grants permission to use the Admin command to open an Admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]

Deletes the account name given by [account_name] from the switch.

edit

Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list

Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is available to all account names without an Admin session.

Notes Authority level or password changes that you make to an account that is currently logged in do not take effect until that account logs in again.

Examples The following is an example of the User Accounts command:

```
SANbox (admin) #> user accounts

    Current list of user accounts
  ----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  chuckca      (admin authority = False, expires in < 50 days)
  gregj        (admin authority = True , expires in < 100 days)
  fred         (admin authority = True , never expires)
```

The following is an example of the User Add command:

```
SANbox (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
SANbox (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
SANbox (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
SANbox (admin) #> user list

  User                          Ethernet Addr-Port    Logged in Since
  ----                          ------------------    --------------
  admin@OB-session1             10.20.68.108-1031     day month date time year
  admin@OB-session2             10.20.68.108-1034     day month date time year
  snmp@OB-session3              Unknown               day month date time year
  snmp@IB-session4              Unknown               day month date time year
  admin@OB-session5             Unknown               day month date time year
```

Whoami

Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
SANbox #> whoami

User name       : admin@session2
Switch name     : SANbox
Switch domain ID: 21 (0x15)
```

Zone

Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning" command on page 13-166 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone

add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [member_list]
rename [zone_old [zone_new]
zonesets [zone]

Keywords

add [zone] [member_list]

Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]

Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]

Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 2000 zones.

delete [zone]

Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all zones and the zone sets of which they are components. This keyword does not require an Admin session.

members [zone]

Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]

Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–239; port numbers can be 0–255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]

Renames the zone given by [zone_old] to the zone given by [zone_new].

zonesets [zone]

Displays all zone sets of which the zone given by [zone] is a component. This keyword does not require an Admin session.

Examples

The following is an example of the Zone List command:

```
SANbox #> zone list

  Zone        ZoneSet
  -------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
SANbox #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
SANbox #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  ----------------------------------
  zone_set_1
```

Zoneset

Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning" command on page 13-166 for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset

activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]

Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active

Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]

Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]

Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]

Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate

Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]

Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list

Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]

Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]

Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]

Displays all zones that are components of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a component of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
SANbox #> zoneset active

  ActiveZoneSet    Bets
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

The following is an example of the Zoneset List command:

```
SANbox #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
SANbox #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the “Zone” command on page 13-159 and the “Zoneset” command on page 13-163.

Authority Admin session except for the Active, History, Limits, and List keywords. The Clear keyword also requires a zoning edit session.

Syntax

zoning
- active
- cancel
- clear
- delete orphans
- edit
- history
- limits
- list
- restore
- save

Keywords

active

Displays information for the active zone set including component zones and zone members. This keyword does not require an Admin session.

cancel

Closes the current Zoning Edit session. Any unsaved changes are lost.

clear

Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword requires a zoning edit session. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

NOTE: The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

delete orphans

Deletes all objects that are not part of the active zone set including zone sets, zones, and aliases.

edit

Opens a Zoning Edit session.

history

Displays a history of zoning modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits

Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This keyword also displays the switch zoning database limits, excluding the active zone set, which are described in Table 13-29. This keyword does not require an Admin session.

Table 13-29. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (2000)
MaxAliases	Maximum number of aliases (2500)
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding those in the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

list

Lists all zoning definitions. This keyword does not require an Admin session.

restore

Restores the volatile zoning database with the contents of the non-volatile zoning database. If the InteropAutoSave parameter is False (see Table 13-8), you can use this keyword to revert changes to the volatile zoning database that were propagated from another switch in the fabric through zone set activation or merging fabrics.

save

Saves changes made during the current Zoning Edit session. The system informs you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
SANbox #> admin start
SANbox (admin) #> zoning edit
SANbox (admin-zoning) #>
.
.
SANbox (admin-zoning) #> zoning cancel

  Zoning edit mode will be canceled.  Please confirm (y/n): [n]   y

SANbox (admin) #> admin end
```

The following is an example of the Zoning Limits command:

```
SANbox #> zoning limits

  Zoning Attribute     Maximum   Current   [Zoning Name]
  ----------------     -------   -------   -------------
  MaxZoneSets          256       6
  MaxZones             2000      17
  MaxAliases           2500      1
  MaxTotalMembers      10000     166
  MaxZonesInZoneSets   2000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 24        Q_1Photon1
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 21        Q_2_NewJBOD2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

The following is an example of the Zoning List command:

```
SANbox #> zoning list
  Active ZoneSet Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
  Configured Zoning Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:16
```

Index

A

account name
  admin 2-2
  display 13-155, 13-158
  factory 3-1
  maintenance mode 3-1
activation
  firmware 5-20, 5-21
  security 9-9, 9-11
  switch configuration 5-11, 5-12
  zoning 7-11
active zone set 7-1, 7-4
Admin
  account name 3-1, 13-1
  authority 2-3, 13-1
  session 2-3
  session timeout 13-93
Admin command 13-4
administrative state
  port 13-83
  switch 13-95
alarm
  configuration 6-10, 13-72
  configuration defaults 13-48
  configuration display 6-4, 13-106
  description 11-1, 13-79
  log 13-59, 13-98
alias
  add members 7-18, 13-5
  copy 7-18, 13-5
  create 7-17, 13-5
  delete 7-17, 13-6
  delete members 13-6
  display list 13-6
  display members 13-6
  information 7-6
  management 7-17
  remove 7-12
  remove ports/devices 7-18
  rename 7-17, 13-6
Alias command 13-5
  Add example 7-18
  Copy example 7-18
  Create example 7-17
  Delete example 7-17
  List example 7-6
  Members example 7-6
  Remove example 7-18
  Rename example 7-17
ALPA - See Arbitrated Loop Physical Address
Arbitrated Loop Physical Address 13-82
authentication 9-1, 10-1, 13-24
authority 3-1, 13-1
authorization 9-1
autosave
  security database 9-7
  zoning database 7-9

B

backup file 5-14
beacon 5-17, 13-60
binding
  fabric 13-23, 13-27
  port 6-8, 13-69
Boot Protocol 13-93
broadcast 13-99

C

Central Processing Unit usage 5-3
certificate 8-1, 8-3, 13-10
Challenge Handshake Authentication Protocol 13-24
CHAP - See Challenge Handshake Authentication Protocol
chassis status 13-99, 13-100

command
  entry 2-3
  examples 13-2
  listing 13-3
  notes 13-2
  reference 13-1
  rules and conventions 13-2
  syntax 13-2
command-line completion 2-3
Config command 13-7
  Activate example 5-11
  Backup example 5-14
  Copy example 5-12
  Delete example 5-12
  Edit example 5-12, 7-9
  List example 5-11
  Restore example 5-16
configuration
  activate 5-11, 13-7
  backup 5-14, 13-7
  copy 5-12, 13-7
  delete 5-12, 13-7
  device security 9-1
  display 5-11
  edit 13-8
  edit session 13-1
  list 13-8
  modify 5-12
  reset 13-43
  restore 5-14, 5-16, 13-8
  save 13-8
configuration file
  download 2-7, 5-15
  upload 2-8
connection
  security 8-1, 13-87, 13-88
  SSL 13-10
CPU - See Central Processing Unit
CRC - See Cyclic Redundancy Check
Create command 13-10
  Certificate example 8-3
  Support example 2-5
credit 6-15, 13-109
critical event 11-1
Cyclic Redundancy Check errors 6-10

D

date 5-17
Date command 5-17, 13-13
decode errors 6-10
default zone 7-9
defaults
  alarm configuration 13-48
  port configuration 13-47
  RADIUS configuration 13-50
  security configuration 13-51
  services configuration 13-50
  SNMP configuration
  switch configuration 13-46
  system configuration 13-51
  zoning configuration 13-49
device
  access 7-1
  security configuration 9-1
discard inactive 7-9
discovery method 4-1
display control 2-4
domain ID
  binding 13-23, 13-27
  display 13-108
donor port 13-109
Dynamic Host Configuration Protocol 13-93

E

elapsed time 5-3
Enterprise Fabric Suite 2007
  license 13-18
errors 6-10
Ethernet
  network information 4-3
  port configuration 4-4

event
  message format 11-2
  output stream control 11-3
  remote logging 11-6
  severity level 11-1
event log
  clear 11-5
  configuration 11-1, 11-4
  configuration management 11-4
  display 11-2
  display configuration 11-5
  filter 11-3
  restore configuration 11-5
event logging
  by component 13-76, 13-114
  by port 13-78, 13-116
  by severity level 13-115
  display 13-114
  remote 11-6
  restore defaults 13-78
  save settings 13-79
  settings 13-116
  severity level 13-78
  start and stop 11-1, 13-79
Exit command 13-14
expiration date 3-1
extended credit 6-15, 13-109
external test 6-12, 13-150

F

fabric
  binding 9-7
  configuration 4-1
Fabric Device Management Interface 13-111
Fabric Security license 13-18
factory defaults 13-44
Fcping command 13-15
  example 4-5
Fctrace command 13-16
  example 4-6
FDMI - See Fabric Device Management Interface
Feature command 13-18
  Add example 5-25
  Log example 5-24
feature upgrade 5-24, 13-18
Fibre Channel
  connection 4-5
  routing 4-6
file download and upload 2-7
File Transfer Protocol
  download files 2-7, 5-15
  download firmware 5-21
  restore configuration file 5-16
  service 13-88
  user account 3-1
firmware 5-21
  custom installation 5-23
  image file 13-34
  information 5-8
  install with CLI 13-20
  installation 5-20
  list image files 13-34
  non-disruptive activation 13-33
  one-step installation 5-21
  remove image files 13-34
  retrieve image file 13-34
  unpack image 13-35
  upload file 2-8
  version 13-147
Firmware Install command 13-20
  example 5-20
FTP - See File Transfer Protocol

G

gateway address 4-1, 4-4, 13-93
Greenwich Mean Time 5-17

group
add members 9-13, 13-23
add to security set 9-11
copy 9-13, 13-25
create 9-12, 13-25
delete 9-12
description 9-1
edit member attributes 13-26
ISL 9-12
list 13-27
list members 13-27
management 9-12
membership 9-5
modify member 9-14
MS 9-12, 13-25
port 9-12
remove from security set 9-11
remove members 9-14, 13-27
rename 9-12, 13-27
type 13-25, 13-27
Group command 13-22
Add example 9-13
Copy example 9-13
Create example 9-12
Delete example 9-12
Edit example 9-14
Members example 9-5
Remove example 9-14
Rename example 9-12
Securitysets example 9-5

H

hard reset 5-20
Hardreset command 13-30
hardware information 5-7
Heartbeat LED 5-7
Help command 2-4, 13-31
History command 13-32
host bus adapter 13-111
hot reset 5-20
Hotreset command 13-33

I

I/O Stream Guard 13-63
Image command 13-34
Install example 5-20
informative event 11-1
internal test 6-12, 13-150
Inter-Switch Link
connection count 6-10
group 9-1, 9-12, 13-25
IP address 4-1, 4-4, 13-93
ISL - See Inter-Switch Link

K

keywords 13-2

L

license key
description 5-24
display 5-24
install 5-25, 13-18
Link Control Frame 13-63
link state database 13-117
Lip command 13-37
log
archive 13-76
clear 13-76
display 13-77, 13-115
event 13-76, 13-114
local 13-93
POST 13-134
remote 13-93
log file 11-7
download 2-7
upload 2-8
logged in users 13-146
login
errors 6-10
limit 2-2
Logout command 13-38

logout errors 6-10
loop port
  bypass 13-82
  enable 13-82
  initialization 13-37
loss-of-signal errors 6-10

M

maintenance mode
  account name 3-1
Management Server
  group 9-1, 9-12, 13-25
  service 13-89
manufacturer information 13-135
mask address 13-93
MD5 authentication 13-24
memory activity 13-122
modify 7-11
MS - See Management Server
Multi-Frame Sequence bundling 13-63

N

name server display 13-123
name server information 4-2
network
  configuration 4-1
  configuration reset 13-45
  discovery 13-93
  discovery method 4-1
  gateway address 13-93
  interfaces 13-113
  IP address 13-93
  mask 13-93
network discovery 4-4
Network Time Protocol
  client 13-94
  description 5-17
  interaction with Date command 13-13
  server address 13-94
  service 13-88
non-disruptive activation 5-21, 13-33
NTP - See Network Time Protocol

O

offline test
  port 6-13
online test 6-12
  port 6-12
operational information 5-2
output stream control 11-3

P

page break 2-4
Passwd command 3-4, 13-39
password
  change 13-39
  default 2-2
  File Transfer Protocol 2-7
  switch 13-39
  user account 3-4
performance tuning 13-63
Ping command 13-40

port
  administrative state 13-83
  binding 6-8, 13-69, 13-104
  configuration 6-1, 13-61
  configuration defaults 13-47
  configuration display 13-101
  configuration parameters 6-2
  counters 13-82
  external test 13-150
  group 9-1, 9-12, 13-25
  information 6-1
  initialize 13-44
  internal test 13-150
  modify operating characteristics 6-7
  online test 13-150
  operational information 6-3, 13-129
  performance 6-5, 13-125, 13-126
  performance tuning 13-63
  reset 6-9
  speed 13-83
  testing 6-12
  threshold alarms 6-4, 6-10
Port Activation license 13-18
POST - See Power-On Self Test
Power-On Self Test log 13-134
preference routing 13-63
process identifier 5-3
processing time 5-3
Ps command 5-3, 13-41

Q

QuickTools 13-88, 13-94
Quit command 13-42

R

RADIUS - Remote Dial-In User Service
RADIUS server
  configuration 8-1, 10-1, 10-3, 13-84
  configuration defaults 13-50
  configuration display 13-136
  information 10-2
  reset 13-44
Registered State Change Notification 13-63
Remote Dial-In User Service 10-1
remote host logging
  description 11-6
  enable 13-93
  host address 13-93
remote logging 4-4
Reset command 13-43
  Config example 7-9
  Factory example 7-9
  Port example 6-9
  Security example 9-9
  SNMP example 12-5
  Zoning example 7-11, 7-12
Reverse Address Resolution Protocol 13-93
routing 13-63, 13-140
RSCN - See Registered State Change Notification

S

SANdoctor license 13-18
secret 13-24
Secure Shell
  description 8-1
  service 8-1, 13-87
Secure Socket Layer
  certificate 8-3, 13-10
  description 8-1
  service 8-1, 13-88
  switch time 13-13

security
  certificate 8-1, 8-3
  configuration 13-67
  configuration defaults 13-51
  configuration display 13-103
  configuration parameters 5-6
  connection 8-1
  database 13-44
  edit session 13-1
  group 9-1
  revert changes 9-7
Security command 13-52
  Activate example 9-9
  Active example 9-4
  Clear example 9-9
  Edit example 9-9
  History example 9-6
  Limits example 9-6
  List example 9-3
  Save example 9-9
security database
  autosave 9-7
  clear 13-52
  configuration 9-7
  description 9-1
  display 13-53
  display history 13-53
  information 9-2
  limits 9-6, 13-53
  modification history 9-6
  modify 9-9
  reset 9-9
  restore 9-7
security edit session
  cancel 13-52
  initiate 13-53
  revert changes 13-53
  save changes 13-53
security set
  activate 9-11, 13-56
  active 9-4
  add group 9-11
  add member group 13-56
  configured 9-2
  copy 9-10, 13-57
  create 9-10, 13-57
  deactivate 9-11, 13-57
  delete 9-10, 13-57
  delete member group 13-57
  description 9-1
  display 13-57
  display active 13-52, 13-56
  display members 13-57
  information 9-2
  management 9-10
  membership 9-5
  remove groups 9-11
  rename 9-10, 13-57
Securityset command 13-56
  Activate example 9-11
  Active example 9-4
  Add example 9-11
  Copy example 9-10
  Create example 9-10
  Deactivate example 9-11
  Delete example 9-10
  Group example 9-5
  List example 9-2
  Remove example 9-11
  Rename example 9-10
services
  configuration defaults 13-50
  display 5-9, 8-3
  managing 5-9
  SNMP 12-1
Set Beacon command 5-17
Set Config Port command 13-61
  example 6-7
Set Config Security command 13-67
  example 9-8
Set Config Security Port command 13-69
  example 6-9

Set Config Switch command 13-70
example 5-13
Set Config Threshold command 13-72
example 6-11
Set Config Zoning command 13-74
example 7-9
Set Log command 13-76
Archive example 11-7
Clear example 11-5
Display example 11-3
example 11-4
Restore example 11-5
Start example 11-1
Stop example 11-1
Set Pagebreak command 13-80
example 2-4
Set Port command 13-82
Set Setup command
SNMP example 12-4
Set Setup Radius command 13-84
example 10-3
Set Setup Services command 13-87
example 5-10
NTP service 5-19
SNMP service 12-2
SSH and SSL services 8-2
Set Setup SNMP command 13-90
Set Setup System command 13-93
Ethernet configuration 4-4
NTP configuration 5-19
remote logging 11-6
Set Switch State command 13-95
Set Timezone command 13-96
severity level 11-1
SHA-1 authentication 13-24
Show About command 13-97
Show Alarm command 13-98
Show Broadcast command 13-99
Show Chassis command 13-100
example 5-7
Show Config Port command 13-101
example 6-2
Show Config Security command 13-103
example 5-6
port binding 6-8
Show Config Security Port command 13-104
Show Config Switch command 13-105
example 5-5
Show Config Threshold command 13-106
example 6-4
Show Config Zoning command 13-107
example 5-6
Show Domains command 13-108
Show Donor command 13-109
example 6-16
Show Fabric command 13-110
example 4-3
Show FDMI command 13-111
Show Interface command 13-113
Show Log command 13-114
display log 11-2
filter display 11-3
Settings example 11-5
Show LSDB command 13-117
Show Media command 13-118
example 6-6
Show Mem command 13-122
Show NS command 13-123
example 4-2
Show Pagebreak command 13-125
Show Perf command 13-126
example 6-5
Show Port command 13-129
example 6-3
Show Post Log command 13-134
Show Setup Mfg command 13-135
Show Setup Radius command 13-136
example 10-2
Show Setup Services command 13-137
example 5-9
SSL and SSH example 8-3
Show Setup SNMP command 13-138
example 12-3
Show Setup System command 13-139
example 4-3
Show Steering command 13-140

Show Switch command 13-141
Show Timezone command 13-143
Show Topology command 13-144
Show Users command 13-146
Show Version command 13-147
  example 5-8
Shutdown command 13-148
Simple Network Management Protocol
  configuration 12-1, 13-90
  configuration display 13-138
  defaults 13-49
  information 12-3
  modify configuration 12-4
  reset 13-44
  reset configuration 12-5
  service 12-1, 13-88
SMI-S - See Storage Management Initiative-Specification
SNMP - See Simple Network Management Protocol
soft
  reset 5-20
  zone 7-1
SSH - See Secure Shell
SSL - See Secure Socket Layer
Storage Management Initiative-Specification 13-88
subnet mask 4-1
support file 13-10
  create 2-5
  download 2-6, 2-7
  upload 2-8
switch
  administrative state 13-95
  configuration 5-1, 5-11, 13-70
  configuration defaults 13-46
  configuration display 13-105
  configuration parameters 5-5, 5-13
  date and time 8-3
  hard reset 13-30
  information 5-1
  log 13-93
  login 2-2
  management service 13-87
  manufacturer information 13-135
  operational information 5-2, 13-141
  paging 5-17
  reset 5-4, 5-20, 13-154
  reset without POST 13-45
  services 5-9, 13-44, 13-87, 13-137
  user accounts 3-1
syntax 13-2
system configuration
  change 13-93
  defaults 13-51
  display 13-139
system process information 5-3

T

technical support 2-5
Telnet
  connection security 8-1
  login 2-2
  service 13-87
  session timeout 13-93
test
  cancel 6-14
  offline 6-13
  online 6-12
  status 6-14
Test Cancel command 13-149
Test command
  example 6-12

Test Port command 13-150
  example 6-12
Test Status command 13-153
TFTP - See Trivial File Transfer Protocol
time
  between resets 5-4
  set and display 5-17, 13-13
  zone 13-96, 13-143
time zone 5-17
timeout
  Admin session 13-93
  admin session 4-4
  inactivity 4-4
  Telnet session 13-93
topology 13-144
transceiver information 6-6
Trivial File Transfer Protocol 5-21

U

Universal Time 5-17
upgrade 5-24, 13-18
Uptime command 13-154
  example 5-4
user account
  add 13-155
  configuration 3-1
  create 3-3
  delete 13-155
  display 13-155
  edit 13-155
  information 3-2
  list 13-155
  logged in 13-146
  modify 3-4
  password 3-4
user administration 13-155
User command 13-155
  Accounts example 3-2
  Add example 3-3
  Delete example 3-4
  Edit example 3-4
  List example 3-2

V

Virtual Interface preference routing 13-63

W

warning 11-1
web applet
  enable 13-94
  service 13-88
Whoami command 13-158
workstation
  date and time 8-3
  settings 2-2

Z

zone
  add member port 13-159
  add to zone set 7-14, 7-16
  copy 7-16, 13-159
  create 7-15, 13-159
  definition 7-1
  delete 7-15, 13-160
  delete member port 13-160
  list 13-160
  list members 13-160
  management 7-15
  membership 7-5
  remove 7-12
  remove from zone set 7-14
  remove ports/devices 7-16
  rename 7-16, 13-160
Zone command 13-159
  Add example 7-16
  Copy example 7-16
  Create example 7-15
  Delete example 7-15
  Members example 7-5
  Remove example 7-16
  Rename example 7-16
  Zonesets example 7-5

zone set
activate 7-14, 13-163
active 7-1, 7-4, 13-166
add member zone 13-163
add zones 7-14
configured 7-2
copy 7-14, 13-163
create 7-13, 13-163
deactivate 7-15, 13-45, 13-164
definition 7-1
delete 7-13, 13-164
delete member zone 13-164
display 13-164
display active 13-163
display members 13-164
display zones 13-160
information 7-2
management 7-13
membership 7-5
remove 7-12
remove zones 7-14
rename 7-14, 13-164
Zoneset command 13-163
Activate example 7-14
Active example 7-4
Add example 7-14
Copy example 7-14
Create example 7-13
Deactivate example 7-15
Delete example 7-13
List example 7-2
Remove example 7-14
Rename example 7-14
Zones example 7-5
zoning
configuration 7-1, 13-74
configuration defaults 13-49
configuration display 13-107
configuration parameters 5-6
database 13-45
edit 13-167
edit session 13-1
hardware enforced 7-1
history 13-167
information 7-2
limits 13-167
list definitions 13-167
modification history 7-7
modify 7-9
reset 7-11
restore 7-9
revert changes 7-9, 13-168
save edits 13-168
Zoning command 13-166
Active example 7-4
Clear example 7-12
Delete example 7-12
Edit example 7-11
History example 7-7
Limits example 7-8
List example 7-3
zoning database 7-11
configuration 7-9
limits 7-8
reset 7-12

Notes